TSM-39

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: T. TERAMURA, et al

Serial No.: 10/811,905

Filed: March 30, 2004

For: ELECTRONIC KEY SYSTEM AND ELECTRONIC KEY USAGE METHOD

Group: 2635

Examiner: W. L. Bangachon

LETTER CLAIMING RIGHT OF PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

April 11, 2006

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, applicants hereby claim the right of priority based on:

Japanese Application No. 2003-118126
Filed: April 23, 2003

A Certified copy of said application document is attached hereto.

Respectfully submitted,

Carl I. Brundidge
Registration No. 29,621
MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

CIB/jdc
Enclosures
703/684-1120

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月２３日

出願番号
Application Number: 特願２００３－１１８１２６

[ST. 10/C]: [ＪＰ２００３－１１８１２６]

出願人
Applicant(s): 株式会社日立製作所

２００４年　３月１５日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

【書類名】　特許願
【整理番号】　HK14920000
【提出日】　平成15年 4月23日
【あて先】　特許庁長官　　殿
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
　【氏名】　寺村　健
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
　【氏名】　齊藤　元伸
【発明者】
　【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　情報・通信グループ内
　【氏名】　桑名　利幸
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社　日立製作所
【代理人】
　【識別番号】　100084032
　【弁理士】
　【氏名又は名称】　三品　岩男
　【電話番号】　045(316)3711
【手数料の表示】
　【予納台帳番号】　011992
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】明細書

【発明の名称】電子鍵システムおよび電子鍵利用方法

【特許請求の範囲】

【請求項１】

電子鍵を利用してサービス提供を行う電子鍵システムにおいて、

電子鍵を識別するための主ＩＤおよび副ＩＤを有する電子鍵データを記憶した利用者モジュールと、サービス提供可否を判定するサービス提供デバイスとを有し、

前記利用者モジュールは、サービス提供デバイスからの電子鍵の送信要求を受け付ける受付手段と、電子鍵データを前記サービス提供デバイスに送信する送信手段を有し、

前記サービス提供デバイスは、サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、利用者モジュールから電子鍵データを受け付ける受付手段と、前記受け付けた電子鍵データの主ＩＤが、前記サービス許可情報に存在するか否かを判定する第１の判定手段と、前記受け付けた電子鍵データの副ＩＤが、前記サービス拒否情報に存在するか否かを判定する第２の判定手段とを有し、

前記サービス提供デバイスは、前記第１および第２の判定結果により、サービス提供可否を判断する提供判断手段とを有すること、

を特徴とする電子鍵システム。

【請求項２】

請求項１に記載の電子鍵システムにおいて、

前記提供判断手段は、前記第１の判定手段において、主ＩＤが前記サービス許可テーブルに存在すると判定し、かつ、前期第２の判定手段において、副ＩＤが前記サービス拒否テーブルに存在しない場合に、サービス提供を許可すること

を特徴とする電子鍵システム。

【請求項３】

請求項１または２に記載の電子鍵システムにおいて、

前記電子鍵データは、電子鍵の共有可能か否かを示す共有階層データを有し、

前記利用者モジュールは、共有階層データが共有可能な場合に、主ＩＤが同一で、かつ副ＩＤが異なる共有用電子鍵を生成する生成手段を有すること

を特徴とする電子鍵システム。

【請求項４】

請求項１、２または３に記載の電子鍵システムにおいて、

前記電子鍵システムは、電子鍵サービスを管理する電子鍵管理装置を有し、

前記電子鍵管理装置は、利用者を識別する会員番号と副ＩＤを含む顧客テーブルを記憶する手段と、外部システムから会員番号および副ＩＤを受け付ける受付手段と、受け付けた会員番号に対応する前記顧客テーブルの副ＩＤと、受付けた副ＩＤとが一致するか否かを判定し、前記判定手段に基づき、同一の主ＩＤを有する利用者モジュールを全て無効化する全体無効化処理を行うか、または、同一の副ＩＤを有する利用者モジュールのみを無効化する部分無効化処理を行うかを判定する無効化判定手段と、前記無効化判定結果を前記サービス提供デバイスに送信する送信手段とを有し、

前記サービス提供デバイスは、前記無効化判定結果に応じて、サービス拒否テーブルまたはサービス許可テーブルの変更を行う変更手段を有すること

を特徴とする電子鍵システム。

【請求項５】

サービス提供を行うサービス提供デバイスが、サービス提供可否を判定するために用いる電子鍵データを記憶した利用者モジュールにおいて、

前記電子鍵データは、電子鍵を識別するための主ＩＤデータおよび副ＩＤデータを有し、

前記利用者モジュールは、前記サービス提供デバイスから電子鍵の送信要求を受け付ける送信要求受付手段と、電子鍵データを前記サービス提供デバイスに送信する送信手段とを有すること

を特徴とする利用者モジュール。

【請求項６】

請求項５に記載の利用者モジュールにおいて、

前記電子鍵データは、電子鍵の共有可能か否かを示す共有階層データを有し、

前記利用者モジュールは、電子鍵の共有要求を受け付ける共有要求受付手段と、

共有可能な場合に、主ＩＤが同一で、かつ副ＩＤが異なる共有用電子鍵データを生成する生成手段と、

前記生成した共有用電子鍵データを、外部システムに送信する送信手段とを有すること

を特徴とする利用者モジュール。

【請求項７】

請求項６に記載の利用者モジュールにおいて、

前記利用者モジュールは、共有階層データが所定の値の場合は共有不可と判断し、共有階層データの値が所定の値以外の場合は共有可能と判定する共有判断手段とを有し、

前記生成手段は、電子鍵データの共有階層データの値を「１」減算した値に変更して共有用電子鍵データを生成すること

を特徴とする利用者モジュール。

【請求項８】

利用者モジュールに記憶された電子鍵データを利用し、サービス提供可否を判定するサービス提供デバイスにおいて、

サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、

利用者モジュールから電子鍵データを受け付ける受付手段と、

前記受け付けた電子鍵データと、前記サービス許可情報と、前記サービス拒否情報とにもとづき、前記受け付けた電子鍵データのサービス提供可否を判断する判断手段と、を有すること、

を特徴とするサービス提供デバイス。

【請求項９】

請求項８に記載のサービス提供デバイスであって、

前記電子鍵データは、電子鍵を識別するための主ＩＤデータおよび副ＩＤデータを有し、

前記判断手段は、前記受け付けた電子鍵データの主ＩＤが、前記サービス許可情報に存在するか否かを判定する第１の判定手段と、前記受け付けた電子鍵データの副ＩＤが、前記サービス拒否情報に存在するか否かを判定する第２の判定手段とを有し、前記第１および第２の判定結果に応じて、前記受け付けた電子鍵データのサービス提供可否を判断すること、

を特徴とするサービス提供デバイス。

【請求項１０】

利用者モジュールに記憶された電子鍵データを利用し、サービス提供可否を判定するサービス提供デバイスにおいて、

前記電子鍵データは、電子鍵を識別するための主ＩＤデータおよび副ＩＤデータを有し、

前記サービス提供デバイスは、サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、

利用者モジュールから電子鍵の一部無効化指示または全体無効化指示を受け付ける無効化受付手段と、

一部無効化指示を受け付けた場合に、前記指示に含まれる主ＩＤデータおよび副ＩＤデータを、前記サービス拒否情報に追加する追加手段と

全体無効化指示を受け付けた場合に、前記指示に含まれる主ＩＤデータを、前記サービス許可情報から削除する削除手段と、を有すること

を特徴とする前記サービス提供デバイス。

【請求項１１】

サービス提供を受けるための電子鍵データを管理する電子鍵管理装置であって、

前記電子鍵管理装置は、電子鍵を識別するための主ＩＤデータと、電子鍵を識別するための副ＩＤデータと、電子鍵の共有可能な範囲を示す共有階層データとを有する電子鍵データを記憶する記憶手段と、

ネットワークで接続された端末装置から入力された副ＩＤデータを含む電子鍵の共有要求を受け付ける共有要求手段と、

共有階層データを参照して共有可能か否かを判定する共有判定手段と、

共有可能な場合に、共有用電子鍵データを生成する生成手段と、を有することを特徴とする電子鍵管理装置。

【請求項１２】

サービス提供を受けるための電子鍵データを管理する電子鍵管理装置であって、

前記電子鍵管理装置は、サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、

外部システムから電子鍵データを受け付ける受付手段と、

前記受け付けた電子鍵データと、前記サービス許可情報と、前記サービス拒否情報にもとづき、前記受け付けた電子鍵データのサービス提供可否を判断する判断手段と、を有すること、

を特徴とする電子鍵管理装置。

【請求項１３】

電子鍵を利用して住宅のドアの開錠または施錠を行うドアの開錠施錠システムにおいて、

電子鍵を識別するための主ＩＤおよび副ＩＤを有する電子鍵データを記憶したＩＣカードと、前記電子鍵データの正当性を判定しドアの開錠または施錠を行うデバイスとを有し、

前記ＩＣカードは、前記デバイスからの電子鍵の送信要求を受け付け、電子鍵データを前記デバイスに送信する送信手段を有し、

前記デバイスは、サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、ＩＣカードから電子鍵データを受け付ける手段と、前記受け付けた電子鍵データの主ＩＤが、前記サービス許可情報に存在するか否かを判定する第１の判定手段と、前記受け付けた電子鍵データの副ＩＤが、前記サービス拒否情報に存在するか否かを判定する第２の判定手段とを有し、

前記デバイスは、前記第１および第２の判定結果により、前記受け付けた電子鍵データの正当性を判断し、ドアの開錠または施錠を行う実行手段と、を有する

こと、

を特徴とするドアの開錠施錠システム。

【請求項１４】

レンタカーの鍵として電子鍵を使用し、レンタカーの鍵を利用者に提供するレンタカーサービスシステムにおいて、

電子鍵を識別するための主ＩＤおよび副ＩＤを有する電子鍵データを記憶したＩＣカードと、前記電子鍵データの正当性を判定してレンタカーの利用を許可するデバイスと、サービス提供を受けるための電子鍵データを管理する電子鍵管理装置とを有し、

前記電子鍵管理装置は、外部システムから選択されたレンタカーを、識別する主ＩＤおよび副ＩＤを有する電子鍵を生成する生成手段と、生成した電子鍵を利用者のＩＣカードに送信する送信手段と、主ＩＤを前記デバイスに送信する送信手段とを有し、

前記ＩＣカードは、前記生成された電子鍵を記憶する記憶手段を有し、

前記デバイスは、前記送信された主ＩＤを、提供を許可するためのサービス許可情報に記憶する記憶手段を有すること

を特徴とするレンタカーサービスシステム。

【請求項１５】

サービス提供可否を判断するサービス提供デバイスが、サービス提供可否を判断するための利用するコンピュータ装置の利用プログラムにおいて

前記コンピュータ装置に、電子鍵を識別するための主ＩＤデータおよび副ＩＤデータを記憶する記憶手段と、

前記サービス提供デバイスから電子鍵の送信要求を受け付ける送信要求受付手段と、電子鍵データを前記サービス提供デバイスに送信する送信手段とを機能させること、

を特徴とする利用プログラム。

【請求項１６】

請求項１５に記載の利用プログラムにおいて、

前記コンピュータ装置に、電子鍵の共有可能か否かを示す共有階層データを記

憶する記憶手段と、

電子鍵の共有要求を受け付ける共有要求受付手段と、

共有可能な場合に、主ＩＤが同一で、かつ副ＩＤが異なる共有用電子鍵データを生成する生成手段と、

前記生成した共有用電子鍵データを、外部システムに送信する送信手段とを機能させること、

を特徴とする利用プログラム。

【請求項１７】

利用者モジュールに記憶された電子鍵データを利用し、サービス提供可否をコンピュータ装置に判断させるサービス提供可否判断プログラムにおいて

コンピュータ装置に、サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、

利用者モジュールから電子鍵データを受け付ける受付手段と、

前記受け付けた電子鍵データと、前記サービス許可情報と、前記サービス拒否情報とにもとづき、前記受け付けた電子鍵データのサービス提供可否を判断する判断手段として機能させること

を特徴とするサービス提供可否判断プログラム。

【請求項１８】

電子鍵を利用しサービス提供を行う電子鍵利用方法において、

サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶ステップと、

外部システムから、電子鍵を識別するための主ＩＤデータおよび副ＩＤデータを含む電子鍵データを受け付ける受付ステップと、

前記受け付けた電子鍵データの主ＩＤが、前記サービス許可情報に存在するか否かを判定する第１の判定ステップと、

前記受け付けた電子鍵データの副ＩＤが、前記サービス拒否情報に存在するか否かを判定するする第２の判定ステップと、

前記第１および第２の判定ステップの結果に応じて、前記受け付けた電子鍵データのサービス提供可否を判断する提供可否判断ステップと、を有すること

を特徴とする電子鍵利用方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＩＣカードなどのデバイスに電子鍵を格納し、各種サービスの提供可否を判定する電子鍵システムおよび電子鍵利用方法に係わり、特に複数の利用者間で電子鍵を共有する電子鍵方法および電子鍵システムに係わる。

【０００２】

【従来の技術】

各種サービスの提供可否を判定する手段として、ＩＣカードに格納された電子鍵を利用するサービス提供方法が開示されている（特許文献１参照）。具体的には、予約したホテルの部屋、あるいは、レンタカーの鍵を電子鍵としてＩＣカードに格納し、サービス提供場所に設置されたサービス提供可否を判断する装置が、該ＩＣカードから電子鍵を読み出し、読み出した電子鍵の情報を正当と判定した場合に、ドアの開錠などを実行する。

【０００３】

また、ＩＣカードから電子鍵を読み出し、電子鍵の情報の正当性を判定してサービス提供の可否を判断する装置についても開示されている（特許文献１および特許文献２参照）。

【０００４】

【特許文献１】

特開２００２－２７９３６０号公報

【特許文献２】

特開平７－２３３６６３号公報

【０００５】

【発明が解決しようとする課題】

上記従来技術では、複数の利用者が電子鍵を共有してサービスを共同利用する方法について開示されていない。また、電子鍵を共有する簡単な方法としては、利用者が保有するＩＣカードに同一の電子鍵をコピーし、電子鍵を共有する方法

が考えられるが、次のような問題が生じる。例えば、同一の電子鍵をコピーしたＩＣカードのうちのいずれかが紛失あるいは盗難した場合、紛失等されたＩＣカードの不正利用を防止するために、当該電子鍵をサービス提供者装置において無効にする必要がある。しかし、同一の複数の電子鍵のうちのいずれか１つを無効にした場合は、他の残りの電子鍵の全てが無効となってしまう。

【０００６】

本発明は上記事情を考慮してなされたものであり、本発明の目的は利用者が共有する電子鍵の一部を無効化した場合であっても、他の電子鍵を必ずしも無効とする必要がないようにすることにある。

【０００７】

【課題を解決するための手段】

上記課題を解決するために、本発明は、利用者の保有するＩＣカードなどの利用者モジュールに、第１の識別子である主ＩＤデータと、第２の識別子である副ＩＤデータから構成される電子鍵データを格納し、サービス利用可否を判定するサービス提供デバイスにおいては、サービス許可テーブルとサービス拒否テーブルの２つのテーブルを保持し、サービス提供デバイスは該電子鍵データの正当性を判断する。

【０００８】

例えば、電子鍵を利用してサービス提供を行う電子鍵システムにおいて、電子鍵を識別するための主ＩＤおよび副ＩＤを有する電子鍵データを記憶した利用者モジュールと、サービス提供可否を判定するサービス提供デバイスとを有する。そして、前記利用者モジュールは、サービス提供デバイスからの電子鍵の送信要求を受け付ける受付手段と、電子鍵データを前記サービス提供デバイスに送信する送信手段を有し、前記サービス提供デバイスは、サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、利用者モジュールから電子鍵データを受け付ける受付手段と、前記受け付けた電子鍵データの主ＩＤが、前記サービス許可情報に存在するか否かを判定する第１の判定手段と、前記受け付けた電子鍵データの副ＩＤが、前記サービス拒否情報に存在するか否かを判定する第２の判定手段とを有し、

前記サービス提供デバイスは、前記第１および第２の判定結果により、サービス提供可否を判断する提供判断手段と有する電子鍵システムを提供する。

【０００９】

【発明の実施の形態】

以下に、本発明に係る第１の実施の形態について説明する。本実施の形態は、住宅のドアの鍵に電子鍵を適用した場合の実施形態である。

【００１０】

図１に、本発明を適用した電子鍵システムのシステム構成図を示す。

【００１１】

図示するように、本実施形態のシステムは、利用者モジュール１００、利用者端末２００、電子鍵管理装置３００およびサービス提供デバイス４００を有する。これらは、インターネットなどのネットワーク５２０により相互に接続される。

【００１２】

利用者モジュール１００は、電子鍵データを格納し、後述する所定の処理に応じて電子鍵データの送信、生成などを行うデバイスである。電子鍵の偽造、不正コピーなどを防止するために、利用者モジュール１００は、ＩＣカードなど耐タンパ性を有するデバイスを用いることが望ましい。

【００１３】

利用者端末２００は、サービスの利用を希望する利用者が保有する端末である。携帯タイプの端末２００は携帯電話網などのネットワーク５１０を介してネットワーク５２０に接続される。

【００１４】

電子鍵管理装置３００は、利用者からの要求に応じて電子鍵を発行、無効化するなどの電子鍵の各種管理を行う。例えば、ＷＥＢサイトなどである。サービス提供デバイス４００は、利用者モジュール１００に格納されている電子鍵の正当性を判定し、その結果に応じてサービス提供可否を判定するデバイスである。本実施形態において、サービス提供デバイス４００は、利用者の住宅のドアに取り付けられ、電磁式ロックなどと接続して電子鍵の正当性を判定し、正当な電子鍵

の場合にドアを開錠または施錠を実行するデバイスである。

【００１５】

次に、電子鍵システムのハードウェア構成について説明する。

【００１６】

図２は、図２に示すように、利用者モジュール１００、利用者端末２００、電子鍵管理装置３００、サービス提供デバイス４００の各装置のハードウェア構成を示したものである。

【００１７】

利用者端末２００は、例えば、プログラムに従ってデータの加工・演算を行なうＣＰＵ９０１と、ＣＰＵ９０１が直接読み書き可能なメモリ９０２と、ハードディスク等の外部記憶装置９０３と、外部システムとデータ通信をするために通信装置９０４と、キーボード、キーボタン、音声入力装置等の入力装置９０５と、ディスプレイまたはプリンタ等の出力装置９０６とを有する一般的なコンピュータシステムを利用することができる。具体的には、携帯電話、利用者簡易携帯電話(PHS: Personal Handy-Phone System)、PDA (Personal Digital Assistant)、PC (Personal Computer) などである。

【００１８】

電子鍵管理装置３００は、前記利用者端末２００と同様の一般的なコンピュータシステムを利用することができる。具体的には、サーバ、ホストコンピュータなどである。

【００１９】

利用者モジュール１００は、図２に示す構成のうち、少なくとも、プログラムに従ってデータの加工・演算を行なうＣＰＵ９０１と、ＣＰＵ９０１が直接読み書き可能なメモリ９０２と、外部システムとデータ通信をするために通信装置９０４とを有するコンピュータ装置であり、例えばＩＣカードなどを利用することができる。

【００２０】

サービス提供デバイス４００は、図２に示す構成のうち、少なくとも、プログラムに従ってデータの加工・演算を行なうＣＰＵ９０１と、ＣＰＵ９０１が直接

読み書き可能なメモリ９０２と、外部システムとデータ通信をするために通信装置９０４とを有するコンピュータ装置である。

【００２１】

次に、電子鍵システムの機能構成について説明する。

【００２２】

図３は、図１に示す各装置の機能構成を示した図である。以下に述べる各装置の各機能は、各メモリ９０２にロードまたは記憶された所定のプログラムを、利用者モジュール１００プログラムの場合は利用者モジュール１００のＣＰＵ９０１が、利用者端末２００用のプログラムの場合は利用者端末２００のＣＰＵ９０１が、電子鍵管理装置３００用のプログラムの場合は電子鍵管理装置３００のＣＰＵが、サービス提供デバイス４００用のプログラムの場合はサービス提供デバイス４００のＣＰＵ９０１が、それぞれ実行することにより、実現される。

【００２３】

利用者モジュール１００は、制御部１８１、記憶部１８２、利用者端末通信部（以下、「ＵＴ通信部」）１８３、および近距離無線通信部１８４を有する。制御部１８１は、利用者モジュール１００内の各部の制御を行う。記憶部１８２は、プログラムおよびデータをメモリ９０２に記憶する。ＵＴ通信部１８３は、通信装置９０４により、利用者端末２００とデータの送受信を行う。そして、近距離無線通信部１８４は、通信装置９０４により、サービス提供デバイス４００または他の利用者モジュール１００と、無線通信によりデータ送受信を行う。このような無線通信の例としては、無線LAN、ISO/IEC14443などがある。なお、利用者端末２００が近距離無線通信部１８４を有し、利用者モジュール１００は利用者端末２００を介してサービス提供デバイス４００などと通信する構成としても良い。

【００２４】

利用者端末２００は、制御部２８１、記憶部２８２、入力部２８３、遠距離無線通信部２８４、表示部２８５および利用者モジュール通信部（以下、「ＵＭ通信部」）２８６を有する。制御部２８１は、利用者端末２００内の各部の制御を行う。記憶部２８２は、プログラムおよびデータを外部記憶装置９０３に記憶す

る。入力部２８３は、入力装置９０５により、利用者からのデータ入力を受け付ける。遠距離無線通信部２８４は、通信装置９０４により、電子鍵管理装置３００または他の利用者端末２００とデータの送受信を行う。表示部２８５は、出力装置９０６により、利用者へデータの表示を行う。そして、UM通信部２８６は、利用者モジュール１００とのデータ送受信を行う。

【００２５】

電子鍵管理装置３００は、制御部３８１、記憶部３８２および通信部３８３を有する。制御部３８１は、電子鍵管理装置３００内の各部の制御を行う。記憶部３８２は、プログラムおよびデータを外部記憶装置９０３に記憶する。通信部３８３は、ネットワーク５２０を介して、通信装置９０４により、利用者端末１００またはサービス提供デバイス２００とデータの送受信を行う。

【００２６】

サービス提供デバイス４００は、制御部４８１、記憶部４８２および通信部４８３、近距離無線通信部２４８を有する。制御部４８１は、サービス提供デバイス４００内の各部の制御を行う。記憶部４８２は、プログラムおよびデータをメモリ９０２に記憶する。通信部４８３は、通信装置９０４により、電子鍵管理装置３００とデータの送受信を行う。近距離無線通信部２４８は、利用者モジュール１００とデータ送受信を行う。

【００２７】

次に、電子鍵システムに用いられる各種のデータのデータ構成図について説明する。

【００２８】

図４は、電子鍵システムに用いられる各種のデータのデータ構成図を示したものである。図示するように、利用者モジュール１００、電子鍵管理装置３００、サービス提供デバイス４００に以下に説明する各種のデータが格納されている。

【００２９】

利用者モジュール１００には、暗号鍵である利用者モジュール認証鍵データ（以下、「UM認証鍵データ」）１１０と、利用者電子鍵テーブル１２０が格納されている。UM認証鍵データ１１０は、後述する相互認証処理において使用され

る暗号鍵データである。暗号鍵データには、例えば共通鍵暗号系における共通鍵を用いることが考えられる。共通鍵暗号系の例としては、DES(Data Encryption Standard)、AES(Advanced Encryption Standard)などがあげられる。

【００３０】

利用者電子鍵テーブル１２０は、利用者が保有する電子鍵の情報が格納されたデータの集合である。利用者電子鍵テーブル１２０は、電子鍵の名前を表す鍵名称、電子鍵を識別するための第１の識別子である主ＩＤ、電子鍵の共有可能な範囲を示す共有階層、電子鍵を識別するための第２の識別子である副ＩＤの履歴とを有する。

【００３１】

鍵名称には、電子鍵の対象となるサービス提供デバイス４００を、利用者が識別するための名称（例えば「ＸＸ宅」など）を設定する。主ＩＤには、発行済みの他の電子鍵と識別するために、他の電子鍵の主ＩＤとは異なる一意性（ユニーク）のあるＩＤを設定する。例えば、電子鍵管理装置３００において、シリアル番号を管理し、電子鍵の発行ごとにその値をカウントアップして、順次カウントアップされた値を設定することが考えられる。

【００３２】

共有階層には、「０」または「１」以上の数値が設定される。「０」の場合は、電子鍵の共有が不可能なことを意味する。また、例えば共有階層に「２」が設定されている場合は、その電子鍵は第１の共有階層として利用者Ａから利用者Ｂに共有が許可され、更に第２の共有階層として利用者Ｂから利用者Ｃに共有が許可される。また共有階層に「１」が設定されている場合は、第１の共有階層として利用者Ａから利用者Ｂへの共有は許可されるが、更に第２の共有階層として利用者Ｂから利用者Ｃへの共有は禁止される。なお、電子鍵の共有が不可能なことを意味する値は「０」に限られず、あらかじめ定めた所定の値であればよい。

【００３３】

副ＩＤは、電子鍵を識別するための第２の識別子であり、副ＩＤ履歴には複数の副ＩＤデータを格納できる。電子鍵管理装置３００が利用者に新たな利用者モジュールを発行または提供する際に、副ＩＤ履歴には、後述する顧客テーブル３

３０の副ＩＤに設定されているデータが設定される。本実施の形態においては、副ＩＤとして、利用者の携帯番号を使用している。

【００３４】

電子鍵管理装置３００には、サービスデバイス認証鍵データ（以下、「ＳＤ認証鍵データ」）３１０、UM認証鍵データ３２０および顧客テーブル３３０が格納されている。ＳＤ認証鍵データ３１０およびUM認証鍵データ３２０は、UM認証鍵データ１１０と同様に相互認証処理で使用される暗号鍵データである。共通鍵暗号系を用いる場合、電子鍵管理装置３００のUM認証鍵データ３２０は、利用者モジュール１００のUM認証鍵データ１１０と同値のデータが設定される。

【００３５】

顧客テーブル３３０は、利用者に関する各種の情報を管理するデータの集合である。顧客テーブル３３０は、利用者を一意に識別する会員番号、利用者を認証するための英数字列などから構成されるパスワード、電子鍵を共有する場合に共有者内で利用者を識別するための副ＩＤ、その利用者に割り当てられた電子鍵を識別するための主ＩＤ、ＳＤアドレスを有する。主ＩＤには、サービスの利用を申し込んだ利用者の利用者モジュール１００に設定された主ＩＤと同一の値を設定する。副ＩＤは、前述の利用者電子鍵テーブル１２０の副ＩＤに最初に設定された副ＩＤデータと同一の値を設定する。なお、サービス本実施の形態において、副ＩＤは携帯電話番号を用いている。ＳＤアドレスは、ネットワーク５２０におけるサービス提供デバイス４００のネットワークアドレスであり、電子鍵管理装置３００がサービス提供デバイス４００に対して、データの送受信を行うために使用される。具体的には、ＩＰアドレスなどが適用される。

【００３６】

サービス提供デバイス４００には、ＳＤ認証鍵データ４１０、UM認証鍵データ４２０、サービス許可テーブル４３０およびサービス拒否テーブル４４０が格納されている。ＳＤ認証鍵データ４１０およびUM認証鍵データ４２０は、UM認証鍵データ１１０等と同様に相互認証処理で使用される暗号鍵データである。共通鍵暗号系を用いる場合、サービス提供デバイス４００のＳＤ認証鍵データ４

１０は、電子鍵管理装置３００のＳＤ認証鍵データ３１０と、同値のデータが設定される。また、サービス提供デバイス４００のＵＭ認証鍵データ４２０は、電子鍵管理装置３００のＵＭ認証鍵データ３２０および利用者モジュール１００のＵＭ認証鍵データ１１０と同値のデータが設定される。

【００３７】

サービス許可テーブル４３０は、サービス提供デバイス４００において、サービスの利用が許可される電子鍵を識別するためのテーブルであり、サービスの利用が許可される主ＩＤのデータを有する。サービス拒否テーブル４４０は、サービス提供デバイス４００において、サービスの利用が禁止される電子鍵を識別するためのテーブルであり、サービスの利用が禁止される主ＩＤおよび副ＩＤのデータを有する。なお、サービス許可テーブル４３０およびサービス拒否テーブル４４０の主ＩＤには、当該サービス提供デバイス４００を利用する利用者モジュールに設定された主ＩＤと同一の値が設定される。

【００３８】

なお、本実施形態においては、図４に示した各種のデータは、サービス拒否テーブル４４０のデータを除き、各装置のメモリ９０２または外部記憶装置９０３にあらかじめ設定されているものとする。例えば、利用者がサービス提供者にサービスの利用を申し込んだタイミングで、電子鍵管理装置３００は各装置のメモリ９０２または外部記憶装置９０３に所定のデータを設定し、利用者モジュール１００、サービス提供デバイス４００などの配布および設置を行う。

【００３９】

次に、図５を参照し、本実施形態において利用者がサービス提供（住宅のドアを開錠する）を受けるときの処理の流れを説明する。

【００４０】

サービス提供デバイス４００の近距離無線通信部４８４は、電子鍵送信要求メッセージを利用者モジュール１００に定期的に送信する（ステップ１０１）。利用者モジュール１００の近距離無線通信部１８４が、該メッセージを受信すると、制御部１８１は、サービス提供デバイス４００の制御部４８１との間で相互認証処理を実行する（ステップ１０２）。該相互認証処理は、例えば、利用者モジ

ュール１００とサービス提供デバイス４００の各々のＵＭ認証鍵データ１１０、４２０を使用し、共通鍵を利用した相互認証手順の規定であるISO/IEC 9798-2に記載の「5.2.2 Three pass authentication」に従って実行される。このような相互認証処理を実行することにより、悪意の第３者が偽の利用者モジュール１００を利用してサービス提供を受けることを防止する。また、偽のサービス提供デバイス４００に対して、利用者モジュール１００が電子鍵を誤って送信し、その結果として電子鍵の内容が露呈することを防止する。

【００４１】

また、該相互認証が終了した後は、セッション鍵などにより、以降の送信メッセージ内容を暗号化することが望ましい。該セッション鍵としては、前記「Three pass authentication」の処理中に生成される乱数を使用する方法がある。このようなメッセージの暗号化を行うことにより、メッセージ盗聴による電子鍵の露呈を防止することが可能である。

【００４２】

次に、利用者モジュール１００の近距離無線通信部１８４は、サービス提供デバイス４００に電子鍵送信メッセージを送信する（ステップ１０３）。該メッセージは、利用者電子鍵テーブル１２０に保持されるデータのうち、少なくとも主ＩＤデータと副ＩＤ履歴データを含むものとする。

【００４３】

サービス提供デバイス４００の近距離無線通信部４８４は、該メッセージを受信し、次に、制御部４８１が受信した主ＩＤデータが、サービス許可テーブル４３０内に存在するか否かを判定する（ステップ１０４）。主ＩＤデータが存在する場合（ステップ１０４でＹＥＳ）は、制御部４８１は、受信した副ＩＤ履歴データに含まれる副ＩＤデータが、サービス拒否テーブル４４０に存在するか否かを判定する（ステップ１０５）。制御部４８１は、この判定において、受信した副ＩＤ履歴データに含まれる副ＩＤデータのうち、一つでもサービス拒否テーブル４４０に存在する場合は、「存在する」と判定する。したがって、サービス拒否テーブル４４０に存在する副ＩＤデータを副ＩＤ履歴に有する利用者鍵テーブルの利用者モジュールは、サービス提供が拒否される。このことにより、該副Ｉ

Ｄから共有を許可された利用者モジュール（該副ＩＤより下位の共有先の利用者モジュール）の使用ができなくなり、紛失または盗難された利用者モジュールから電子鍵をコピーするなど、悪用されることを防止することが可能となる。

【００４４】

副ＩＤが存在しないと判定した場合（ステップ１０５でＮＯ）は、制御部４８１はサービス提供を許可する処理を実行する（ステップ１０６）。本実施形態においては、住居のドアの開錠処理を実行する。

【００４５】

また、副ＩＤが存在すると判定した場合（ステップ１０５でＹＥＳ）は、制御部４８１はサービス提供を拒否し処理を終了する（ステップ１０７）。本実施形態においては、住居のドアの開錠処理を実行せずに施錠したままとする。また、主ＩＤがサービス許可テーブルに存在しない場合（ステップ１０４でＮＯ）の場合も、制御部４８１はサービス提供を拒否し処理を終了する（ステップ１０７）。

【００４６】

上記の処理は、利用者モジュール１００が電子鍵を近距離無線通信１８４により送信する方式について説明したが、他の方式により送信しても良い。例えば、ネットワーク５１０およびネットワーク５２０を経由して送信するようにしても良い。この場合の処理の流れを以下に説明する。本処理は、図５の処理を比較すると、電子鍵送受信処理（ステップ１０１からステップ１０３）の部分においてのみ異なり、他の部分は図５の処理と同じであるため、相違する部分について図６を参照し説明する。

【００４７】

図６は、利用者端末２００を利用して、利用者がサービス提供を受けるときの電子鍵送受信処理の流れを示したものである。

【００４８】

利用者端末２００の入力部２８３が、利用者の操作指示を受け付けると、ＵＭ部２８６は電子鍵送信要求メッセージを利用者モジュール１００に送信する（ステップ２０１）。利用者モジュール１００のＵＴ通信部１３８が、該メッセージ

を受信すると、制御部１８１は、サービス提供デバイス４００の制御部４８１との間で相互認証処理を実行する（ステップ２０２）。該相互認証処理は、利用者端末２００、ネットワーク５１０およびネットワーク５２０を介して実行する。該相互認証処理において使用する認証鍵データ、相互認証手順、その後のメッセージの暗号化などについては、図５のステップ１０２の処理と同様である。

【００４９】

次に、利用者モジュール１００のＵＴ通信部１３８は、サービス提供デバイス４００に電子鍵送信メッセージを送信する（ステップ２０３）。該メッセージ送信において、利用者端末２００、ネットワーク５１０などを介す点は、ステップ２０２と同様である。ステップ２０３の処理の後は、図５に記載されているステップ１０４以降の処理を、サービス提供デバイス４００が実行する。

【００５０】

このような各種ネットワークを介した電子鍵の送信を行うことにより、例えば、電子鍵である利用者モジュール１００を保有する利用者が、外出して自宅にいないときに、知人が自宅を訪問した場合、利用者端末２００から遠隔で自宅のドアの開錠を実行して知人に自宅で待ってもらう、というケースに対応できる。

【００５１】

次に、サービス利用者の間で、電子鍵を共有する場合の処理について説明する。図７は、電子鍵の共有処理の流れを示し、図１１は、共有処理において利用者端末２００に表示される表示画面の例を示したものである。本処理においては、電子鍵の共有元となる利用者が保有する利用者モジュール１００および利用者端末２００を、第１の利用者モジュール１００および第１の利用者端末２００とする。また、電子鍵の共有先の利用者が保有する利用者モジュール１００および利用者端末２００を、第２の利用者モジュール１００および第２の利用者端末２００とする。また、図１１の表示画面の例では、副ＩＤに携帯電話番号を使用している。

【００５２】

まず初めに、第１の利用者端末２００の入力部２８３が、共有元の利用者の操作指示を受け付けると、ＵＭ通信部２８４が電子鍵一覧要求メッセージを第１の

利用者モジュール１００に送信する（ステップ３０１）。第１の利用者モジュール１００のＵＴ通信部１８３は該メッセージを受信し、次に制御部１８１が利用者電子鍵テーブル１２０に格納されている各レコードの鍵名称データおよび主ＩＤデータのペアを、格納レコードの数だけ電子鍵一覧応答メッセージに設定する。そしてＵＴ通信部１８３は、第１の利用者端末２００に電子鍵一覧応答メッセージを送信する（ステップ３０２）。

【００５３】

第１の利用者端末２００のＵＭ通信部２８４は該メッセージを受信し、表示部２８５が受信した鍵名称データの一覧を出力装置９０６に表示する（画面３１）。そして、第１の利用者端末２００の入力装置９０５は、利用者が選択データの一覧から選択した鍵名称の選択指示を受け付ける（ステップ３０３）。

【００５４】

次に、第１の利用者端末２００の表示部２８５は、副ＩＤデータ入力画面を出力装置９０６に表示する（画面３２）。そして入力装置９０５は、利用者の入力した副ＩＤデータを受け付ける。副ＩＤデータは、利用者モジュール１００が紛失あるいは盗難された場合に、該利用者モジュール１００の電子鍵のみを無効化するために必要なデータであり、電子鍵を共有する利用者のグループの中で一意となるデータを用いるものとする。本実施形態においては、利用者の電話番号を副ＩＤとして使用する。そしてＵＭ通信部２８４は、共有開始メッセージを第１の利用者モジュール１００に送信する（ステップ３０４）。該メッセージは、ステップ３０３で選択された主ＩＤデータと、ステップ３０４で入力された副ＩＤデータを含む。該メッセージを送信した後、第１の利用者端末２００の表示部２８５は、「コピー処理中」の画面を出力装置９０６に表示する（画面３３）。

【００５５】

第１の利用者モジュール１００のＵＴ通信部１８３は該メッセージを受信し、制御部１８１が共有先の第２の利用者モジュール１００に送信する利用者電子鍵テーブル１２０のデータを生成する（ステップ３０５）。利用者電子鍵テーブル１２０は、図４で説明したデータの集合である。主ＩＤには共有開始メッセージに含まれる主ＩＤデータを設定し、鍵名称には該主ＩＤデータから特定されるレ

コードの鍵名称を設定する。共有階層には、該レコードの共有階層の値から１を引いた値を設定する。ただし、引いた後の値がマイナスの数値となる場合は、これ以上の電子鍵の共有は許可されていないと判定し、以降の処理を実行せずに処理を終了する。副ＩＤ履歴データには、共有開始メッセージに含まれる副ＩＤデータを追加して設定する。

【００５６】

次に、第１の利用者モジュール１００と、第２の利用者モジュール１００は、相互認証処理を実行する（ステップ３０６）。この相互認証処理で使用する認証鍵としては、各々の利用者モジュールが保持するＵＭ認証鍵データ１１０を使用する。また、該相互認証処理は各々の利用者端末２００およびネットワーク５１０を介して行われる。なお、該相互認証処理は、各々の近距離無線通信部１８４を介し、第１の利用者モジュール１００と第２の利用者モジュール１００との間で直接行うこととしても良い。その他の該相互認証処理については、図５のステップ１０２と同様であり、また、以降のメッセージ暗号化についても同様である。

【００５７】

次に、第１の利用者モジュール１００は、電子鍵書込メッセージを第２の利用者モジュール１００に送信する（ステップ３０７）。このとき、該メッセージの送信経路についてはステップ３０６の場合と同様である。該メッセージは、ステップ３０５で生成した利用者電子鍵テーブル１２０のデータを含む。第２の利用者モジュール２００は、電子鍵書込メッセージを受信し、該メッセージ中の利用者電子鍵テーブル１２０のデータ（レコード）を、既存の利用者電子鍵テーブル１２０に追加する（ステップ３０８）。本処理が終了した後、第１の利用者端末２００の表示部２８５は、「コピー終了」の画面を出力装置９０６に表示する（画面３４）。以上により、電子鍵の共有処理を終了する。

【００５８】

次に、電子鍵の共有処理における利用者電子鍵テーブル１２０について説明する。図８は、第１の利用者モジュール１００の利用者電子鍵テーブル１２１（以下、「第１の利用者電子鍵テーブル」）に設定された共有階層の値が「１」のと

きの第１の利用者モジュール１００と、第２の利用者モジュール１００の利用者電子鍵テーブル１２２（以下、「第２の利用者電子鍵テーブル」）を示したものである。

【００５９】

第１の利用者電子鍵テーブル１２１は、電子鍵の共有処理の前後において、データの変更はない。第２の利用者電子鍵テーブル１２２には、鍵名称、主ＩＤが第１の利用者電子鍵テーブル１２１と同じ値が設定され、共有階層に第１の利用者電子鍵テーブル１２１の値から「１」を引いた値「０」が設定され、副履歴ＩＤには第１の利用者端末２００から入力さえた携帯番号が設定されたレコートが新規に追加される。この場合、第２の利用者鍵テーブルの共有階層は「０」であるため、第２の利用者は電子鍵の共有処理を行うことはできない。

【００６０】

図９は、共有元である第１の利用者電子鍵テーブル１２１の共有階層が「３」のときの、第１の利用者電子鍵テーブル１２１、第２の利用者電子鍵テーブル１２２、第３の利用者電子鍵テーブル１２３（第３の利用者モジュール１００の利用者電子鍵テーブル）、第４の利用者電子鍵テーブル１２４（第４の利用者モジュール１００の利用者電子鍵テーブル）示したものである。

【００６１】

第２の利用者電子鍵テーブル１２２には、共有階層に第１の利用者電子鍵テーブル１２１の値から「１」を引いた値「２」が設定され、その他は図８と同様のレコートが新規に追加される。次に、第３の利用者電子鍵テーブル１２３には、共有階層が第２の利用者電子鍵テーブル１２２の値から「１」を引いた値「１」が設定され、副履歴ＩＤには第２の利用者電子鍵テーブル１２２に設定された携帯番号と第２の利用者端末２００から入力さえた携帯番号とが設定されたレコートが新規に追加される。次に第３の利用者電子鍵テーブル１２４には、同様に、共有階層に「０」が、副履歴ＩＤには３つの携帯番号が設定されたレコードが新規に追加される。この場合、第４の利用者鍵テーブルの共有階層は「０」であるため、第４の利用者は電子鍵の共有処理を行うことはできない。

【００６２】

次に、図１０および図１１を参照し、電子鍵を無効化するときの処理の流れを説明する。電子鍵を無効化する場合としては、利用者モジュール１００の紛失または盗難などがあげられる。なお、ステップ４０１からステップ４０５については、既存のＷＥＢブラウザおよびＷＥＢサーバなどで実現可能な処理であるため、詳細な説明は省略する。また、図１１の表示画面の例では、副ＩＤに携帯電話番号を使用している。

【００６３】

まず初めに、利用者端末２００の表示部２８５が、利用者の操作指示に応じ、会員番号およびパスワードの入力を受け付ける画面を表示し（画面４１）、利用者から会員番号およびパスワードの入力を受け付け、遠距離無線通信部２８４がログイン要求メッセージを電子鍵管理装置３００に送信する（ステップ４０１）。ログイン要求メッセージには、利用者から入力された会員番号およびパスワードのデータを含む。電子鍵管理装置３００の通信部３８３が該メッセージを受信すると、制御部３８１は顧客テーブル３３０を検索し、該当会員番号が存在し、かつパスワードが一致するか否かを判定する。会員番号が存在し、パスワードが一致する場合は、通信部３８３は、サービスのメニュー表示メッセージを利用者端末２００に送信する（ステップ４０２）。会員番号が存在しなかった場合、あるいはパスワードが不一致だった場合は、制御部３８１は以降の処理を行わず処理を終了する。なお、該メニュー表示メッセージは、メニュー画面を利用者端末２００の出力装置９０６に表示させるための、コマンド識別子あるいはページ記述言語を含む。このようなページ記述言語としては、例えばＨＴＭＬ（Hyper Text Markup Language）がある。

【００６４】

利用者端末２００の遠距離無線通信部２８４は、メニュー表示メッセージを受信し、表示部２８５は出力装置９０６にメニュー選択画面（画面４２）を表示する。そして、入力部２８３が、入力手段９０５により入力された利用者のメニュー選択を受け付け、その結果を遠距離無線通信部２８４が選択メニューメッセージとして電子鍵管理装置３００に送信する（ステップ４０３）。電子鍵管理装置３００の通信部３８３が該メッセージを受信し、制御部３８１は該メッセージが

登録無効（無効化処理）のメニューを選択していると判定した場合は、副ＩＤ入力要求メッセージを利用者端末２００に送信する（ステップ４０４）。なお、本実施形態においては、無効化処理以外のサービスメニューは無いものとする。

【００６５】

利用者端末２００の遠距離無線通信部２８４は、副ＩＤ入力要求メッセージを受信し、表示部２８５は出力装置９０６に副ＩＤ入力受付画面（画面４３）を表示する。そして、入力部２８３が、入力手段９０５により入力された副ＩＤデータを受け付け、遠距離無線通信部２８４が副ＩＤ登録メッセージを電子鍵管理装置３００に送信する（ステップ４０５）。該メッセージには入力された副ＩＤデータを含む。なお、該メッセージ送信後、利用者端末２００の出力装置９０６には、「無効化登録中」画面（画面４４）が表示される。

【００６６】

電子鍵管理装置３００の通信部３８３が副ＩＤ登録メッセージを受信した後、制御部３８１はサービス提供デバイス４００との間で相互認証処理を実行する（ステップ４０６）。このとき、認証鍵としては電子鍵管理装置３００とサービス提供デバイス４００の各々のＳＤ認証鍵データ３１０、４１０を使用する。また、通信対象となるサービス提供デバイス４００のネットワークアドレスは、ログインされた会員番号データから特定される、顧客テーブル３３０のＳＤアドレスデータとする。その他については、図５のステップ１０２の相互認証処理と同様である。

【００６７】

次に、電子鍵管理装置３００の制御部３８１は、ログイン処理（ステップ４０２）で受信した会員番号データをキーとして顧客テーブル３３０を検索し、該当会員番号の副ＩＤ（携帯電話番号）データを取得する。そして、制御部３８１は、利用者端末２００から受信した副ＩＤ登録メッセージに含まれる副ＩＤデータと、前記電話番号が一致するか否かを判定する（ステップ４０７）。受信した副ＩＤデータが、顧客テーブルの副ＩＤデータと一致する場合は、共有元となる利用者モジュールが紛失または盗難等による無効化であるため、該利用モジュールの主ＩＤを有する電子鍵の全てを無効化する全体無効化処理を行う。一方、受信

した副ＩＤデータが、顧客テーブルの副ＩＤデータと一致しない場合は、利用元以外の利用者モジュール（すなわち利用先の利用者モジュール）であるため、当該副ＩＤを有する利用モジュールのみを無効化する部分無効化処理を行う。この部分無効化処理により、当該副ＩＤを有する利用モジュールから電子鍵の共有を許可された利用モジュールも無効化され、紛失等された利用モジュールの悪用を防止することができる。

【００６８】

部分無効化処理としては、電子鍵管理装置３００の通信部３８３は、サービス提供デバイス４００に追加要求メッセージを送信する（ステップ４０８）。該メッセージは、該当会員番号のレコードの主ＩＤデータと、受信した副ＩＤ登録メッセージ内の副ＩＤデータを含む。サービス提供デバイス４００の通信部４８３は該追加要求メッセージを受信し、制御部４８１が、主ＩＤデータと副ＩＤデータを一つのレコードとしてサービス拒否テーブル４４０に追加する（ステップ４０９）。なお、部分無効化処理（ステップ４０９）を実行した場合は、次に述べる全体無効化処理（ステップ４１０）を実行せずに、無効化終了通知（ステップ４１２）を実行する。

【００６９】

全体無効化処理として、電子鍵管理装置３００の通信部３８３は、サービス提供デバイス４００に削除要求メッセージを送信する（ステップ４１０）。該メッセージは、該当会員番号のレコードの主ＩＤデータを含む。サービス提供デバイス４００の通信部４８３は該削除要求メッセージを受信し、制御部４８１が、サービス許可テーブル４３０から該当する主ＩＤデータを削除する（ステップ４１１）。

【００７０】

部分無効化処理または全体無効化処理を終了した後、電子鍵管理装置３００の通信部３８３は、利用者端末２００に無効化終了通知メッセージを送信する（ステップ４１２）。利用者端末２００の遠距離無線通信部２８４は、該メッセージを受信し、表示部２８５は出力装置９０６に「無効化終了」画面（画面４５）を表示する。

【００７１】

以上により、電子鍵を無効化するときの処理を終了する。

【００７２】

なお、本実施形態において、サービス提供デバイス４００に格納する副ＩＤデータ、あるいはサービス提供デバイス４００に送信されるメッセージに含まれる副ＩＤデータは、暗号化あるいは一方向関数でダイジェスト化するようにしても良い。このような構成にした場合、サービス提供デバイス４００が盗難され、その内部を解析されることにより副ＩＤデータが露呈する（例えば電話番号を副ＩＤデータとして利用していた場合、電話番号が露呈する）ことを防止できる。なお、一方向関数の例としては、SHA-1(Secure Hash Algorithm 1)、MD5(Message Digest 5)などがある。暗号化手段の例としては、DES(Data Encryption Standard)、AES(Advanced Encryption Standard)などの共通鍵暗号系や、楕円曲線暗号などの公開鍵暗号系がある。

【００７３】

また、本実施形態において、副ＩＤデータは利用者端末２００から利用者が入力するようにしていたが、あらかじめ共有元の利用者の利用者端末２００あるいは利用者モジュール１００に格納しておいても良い。この場合、電子鍵共有処理（図７参照）の共有鍵生成処理（ステップ３０５）においては、利用者端末２００からの副ＩＤの入力は不要となり、このあらかじめ格納しておいた副ＩＤデータを、共有用電子鍵データの生成に使用する。あるいは、共有先の利用者の利用者端末２００または利用者モジュール１００に、副ＩＤデータを格納しておいても良い。この場合、電子鍵共有処理（図７参照）の共有鍵生成処理（ステップ３０５）においては、副ＩＤ履歴データに新たに副ＩＤデータを生成せず、電子鍵書込処理（ステップ３０８）において、該格納済み副ＩＤデータを利用者電子鍵テーブル１２０の副ＩＤ履歴に追加する。

【００７４】

次に、本発明に係る第２の実施の形態について説明する。

【００７５】

本実施形態は、レンタカーのドアに電子鍵を適用した場合の形態である。なお

、第１の実施形態と同様な点も多いので、以下に述べる説明は相違点を中心として行う。

【００７６】

本実施形態のシステム構成は、第１の実施形態の場合とほぼ同様である（図１参照）。ただし、本実施形態においてサービス提供デバイス４００は、レンタカーのドアに取り付けられ、電子鍵データの正当性判定に応じてドアの開錠を実行するデバイスとする。あるいは、レンタカーの近傍に設置され、レンタカーの固定装置を前記正当性判定に応じて解除するデバイスであっても良い。

【００７７】

また、ハードウェア構成および機能構成についても、第１の実施形態の場合（図２、図３参照）とほぼ同様である。

【００７８】

次に、本実施形態における電子鍵システムに用いられる各種のデータのデータ構成を、図１２に示す。各種のデータのデータ構成は、第１の実施形態と同様な点は省略し、相違する点について次に説明する。

【００７９】

電子鍵管理装置３００の顧客テーブル３３０は、主ＩＤデータとＳＤアドレスデータをデータ項目として有しない点で、第１の実施形態における顧客テーブル３３０と相違する。また、第１の実施形態では、利用者と、その利用者が利用するサービス提供デバイス（利用者の住宅のドアに取り付けられ電子鍵の正当性を判定するデバイス）は、あらかじめ固定されているため、主ＩＤは会員番号に１対１に対応して設定されていた（図４の顧客テーブル３３０参照）。しかしながら、本実施形態では、利用者と利用者が利用するレンタカーとの関係は、あらかじめ固定されていない。そのため、利用者がレンタカーを選択し、レンタカーの鍵を購入するタイミングで、利用者とレンタカーとを対応付ける必要がある。そのため、本実施形態の電子鍵管理装置３００には、第１の実施形態にはない新たなテーブルとして、取引テーブル３４０および商品テーブル３５０を有する。

【００８０】

取引テーブル３４０は、電子鍵の購入取引を管理するテーブルであり、個々の

電子鍵を識別するための主ＩＤ、該主ＩＤの電子鍵に対応する商品を識別するための商品ＩＤ、該主ＩＤの電子鍵の購入者を識別するための会員番号を有する。取引テーブル３４０は、利用者がレンタカーの鍵を購入するタイミングで、レコードが作成され、取引テーブルに追加さる。

【００８１】

商品テーブル３５０は、サービス提供者が提供する商品を管理するテーブルであり、商品（本実施形態においてはレンタカー）を一意に識別する商品ＩＤ、商品の名称を表す商品名、該商品と対応するサービス提供デバイス４００のネットワークアドレスであるＳＤアドレスを有する。

【００８２】

なお、本実施形態において図１２に示したテーブルおよびデータは、次の４つのテーブルを除き、各装置のメモリ９０２または外部記憶装置９０３にあらかじめ設定されているものとする。その４つのテーブルとは、利用者電子鍵テーブル１２０、取引テーブル３４０、サービス許可テーブル４３０、サービス拒否テーブル４４０である。

【００８３】

次に図１３および図１４を参照し、利用者が電子鍵を購入するときの処理の流れを説明する。図１３は処理フロー図で、図１４は利用者端末の表示画面例であり、本表示画面の例では、副ＩＤに携帯電話番号を使用している。なお、基本的に各メッセージの送受信、相互認証処理など、第１の実施形態と同様である。

【００８４】

利用者端末２００は「会員番号・パスワード入力画面」（画面５１）から入力された会員番号およびバスワードを電子鍵管理装置４００に送信する（ステップ５０１）。電子鍵管理装置４００は、会員番号およびバスワードの入力を受信し、顧客テーブル３３０を参照してログイン処理を実行し、メニュー画面（画面５２）を利用者端末２００に送信する（ステップ５０２）。これらの処理は、第１の実施形態の無効化処理（図１０、図１１参照）と同様である。ただし、メニューとして表示する内容は、画面５２（図１４）と画面４２（図１１）とで異なる。

【００８５】

次にメニュー画面（画面５２）において、「商品購入」メニューが選択された場合の処理の流れについて以下に説明する。なお、「無効登録」が選択された場合に実行される電子鍵無効化処理については後述する。

【００８６】

利用者端末の入力部２８３は、「商品購入」メニューの選択を受け付け、遠距離無線通信部２８４は選択メニューの情報を電子鍵管理装置に送信する（ステップ５０３）。電子鍵管理装置３００の通信部が該メッセージを受け付けると、制御部３８１は商品テーブル３５０を検索し、商品ＩＤデータと商品名データのペアを複数個取得し、通信部３８３はこれを利用者端末２００に送信する（ステップ５０４）。利用者端末２００の遠距離無線通信部２８４は、該データを受信し、表示部２８５は受信データに基づき商品一覧画面（画面５３）を出力装置９０６に表示し、利用者の商品選択の入力を受け付ける（ステップ５０５）。その後、利用者端末２００の入力部２８３が受け付けた商品の商品ＩＤデータを、遠距離無線通信部２８４が電子鍵管理装置３００に送信し、その後、出力装置９０６にダウンロード処理中画面（画面５４）が表示される。

【００８７】

電子鍵管理装置３００の通信部３８３が該商品ＩＤデータを受信した後に、制御部３８１は、利用者モジュール１００と相互認証処理を実行する（ステップ５０６）。認証鍵としては、電子鍵管理装置３００のＵＭ認証鍵データ３１１と利用者モジュール１００のＵＭ認証鍵データ１１０を使用する。

【００８８】

次に、電子鍵管理装置３００の制御部３８１は、主ＩＤデータと副ＩＤデータの生成処理を行う（ステップ５０７）。主ＩＤデータとしては、他の発行済み電子鍵と区別するために、それらの電子鍵の主ＩＤデータとは異なる一意のデータ値を用いる。例えば、電子鍵管理装置３００においてシリアル番号を管理し、電子鍵の発行ごとにその値をカウントアップし、その値を用いることが考えられる。副ＩＤデータには、発行した電子鍵を共有する利用者のグループ内で一意となるデータ値を設定すれば良く、本実施形態では利用者の携帯電話番号を使用する

。

【００８９】

次に電子鍵管理装置３００の制御部３８１は、鍵名称データ、主ＩＤデータ、共有階層データ、副ＩＤ履歴データを有する電子鍵データを生成する（ステップ５０８）。鍵名称データには、ステップ５０５で受信した商品ＩＤデータを検索キーとして特定された商品テーブル３５０の商品名データを設定する。主ＩＤデータおよび副ＩＤ履歴データには、ステップ５０７で生成された主ＩＤデータおよび副ＩＤデータをそれぞれ設定する。共有階層データには、第１の実施形態と同様に、その電子鍵の共有可能な範囲を表す所定の数値データを設定する。そして、電子鍵管理装置３００の制御部３８１は、取引テーブル３４０に今まで説明した主ＩＤデータ、商品ＩＤデータ、および会員番号データを有するレコードを新規に追加する。

【００９０】

次に、電子鍵管理装置３００の制御部３８１は、サービス提供デバイス４００との間で相互認証処理を実行する（ステップ５０９）。認証鍵としては電子鍵管理装置３００のＳＤ認証鍵データ３１０およびサービス提供デバイス４００のＳＤ認証鍵データ４１０を使用する。通信対象とするサービス提供デバイス４００のネットワークアドレスは、商品テーブル３５０における対応ＳＤアドレスデータを設定する。該対応ＳＤアドレスデータは、ステップ５０５で受信した商品ＩＤデータを検索キーとして特定する。

【００９１】

次に、電子鍵管理装置３００の通信部３８３は、ステップ５０７で生成した主ＩＤデータを含む登録要求メッセージを、サービス提供デバイス４００に送信する（ステップ５１０）。

【００９２】

サービス提供デバイス４００の通信部４８３は、該登録要求メッセージを受信し、制御部はサービス許可テーブル４３０に受信した主ＩＤデータを追加する（ステップ５１２）。

【００９３】

次に、電子鍵管理装置３００の通信部３８３は、ステップ５０８で生成した電子鍵データを含む電子鍵書込メッセージを、利用者端末２００のＵＭ通信部２８６を経由して、利用者モジュール１００に送信する（ステップ５１１）。利用者モジュール１００のＵＴ通信部１８３は電子鍵データを受信し、制御部１８１が該電子データを利用者電子鍵テーブル１２０に追加する（ステップ５１３）。その後、利用者端末２００の出力装置９０６には終了画面（画面５５）が表示される。

【００９４】

以上により、利用者が電子鍵を購入するときの処理を終了する。本処理により、利用者があらかじめ固定されていない任意のサービス提供デバイスを利用する場合であっても、電子鍵を利用したサービスの提供（レンタカーの鍵の購入）を受けることが可能である。

【００９５】

電子鍵利用処理および電子鍵共有処理については、第１の実施形態の場合（図５、６、７参照）と同様である。なお、電子鍵共有処理における利用者端末２００の表示画面については、図１４に示すとおりである。

【００９６】

電子鍵無効化処理については、第１の実施形態の場合（図１０参照）と以下の点で相違する。相互認証処理（ステップ４０６）の通信対象とするサービス提供デバイス４００のネットワークアドレスは、本実施形態においてはログイン処理（ステップ５０２）で受信した会員番号データから特定した商品テーブル３５０のＳＤアドレスデータとする。具体的には、会員番号データを検索キーとして取引テーブル３４０から商品ＩＤを特定し、該商品ＩＤを検索キーとして商品テーブル３５０のＳＤアドレスデータを特定する。

【００９７】

また、部分無効化処理（ステップ４０８）および全体無効化処理（ステップ４１０）で送信するメッセージに含まれる主ＩＤデータは、ログイン処理（ステップ４０２）で受信した会員番号データを検索キーとして取引テーブル３４０を検索し取得する。なお、電子鍵無効化処理における利用者端末２００の表示画面に

ついては、図１４に示すとおりである。

【００９８】

以上により、本発明に係る第２の実施の形態について説明した。本処理により、利用者があらかじめ固定されていない任意のサービス提供デバイスを利用する場合であっても、第１の実施形態と同様に、同一の主ＩＤを有する利用者モジュールの全部を無効化する全体無効化処理だけでなく、該当する副ＩＤを有する利用者モジュールのみを無効化する部分無効化処理が可能である。

【００９９】

以上説明したように本発明によれば、複数の利用者で電子鍵を共有してサービスを共同利用する場合において、盗難や紛失などの理由により誰かの電子鍵を無効化する場合でも、必ずしも全ての電子鍵を無効化する必要はなくなる。つまり、利用者の一人が電子鍵を紛失し（あるいは盗難され）、その電子鍵を無効化すると、その利用者と電子鍵を共有していた利用者の全員が必ずサービスの利用を拒否されるという事態を、防止することが可能となる。

【０１００】

なお、本発明は上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。例えば、レンタル会議室の電子鍵、ホテルの部屋の電子鍵、電子ロッカーの電子鍵などがある。

【０１０１】

例えば、第１の実施の形態の利用処理においては、サービス提供デバイス４００がサービス許可テーブル４３０およびサービス拒否テーブル４４０を有し、サービス提供可否の判断を行っている。しかしながら電子鍵管理装置３００が、各サービス提供デバイス４００のサービス許可テーブル４３０およびサービス拒否テーブル４４０を保持し、サービス提供可否の判断を行うこととしてもよい。具体的には、図５における電子鍵送信（ステップ１０３）の送信先を、電子鍵管理装置３００とし、電子鍵管理装置３００がサービス提供可否判断（ステップ１０４～ステップ１０７）を行い、その判断結果をサービス提供デバイス４００に送信することが考えられる。

【０１０２】

また、第１の実施の形態の共有処理においは、利用者モジュール１００が利用者電子鍵テーブル１２０を有し、共有用電子鍵データを生成している。しかしながら、電子鍵管理装置３００が、各利用者モジュールの利用者電子鍵テーブル１２０を保持し、一元管理して、利用者端末からの共有要求に応じて、共有用電子鍵データの生成をおこなうこととしてもよい。具体的には、図７における第１の利用者端末２００の電子鍵一覧取得（ステップ３０１）の送信先を、電子鍵管理装置３００とし、それ以降の第１の利用者モジュール１００の処理（電子鍵一覧応答、共有用電子鍵生成等）を電子鍵管理装置３００が行うことが考えられる。

【０１０３】

【発明の効果】

以上のように、本発明によれば、複数の利用者で電子鍵を共有してサービスを共同利用することが可能となる。また、共有する電子鍵を無効にする場合に、全ての共有する電子鍵を無効にするだけでなく、一部の電子鍵のみを無効にすることが可能となる。

【図面の簡単な説明】

【図１】　本発明の第1の実施形態におけるシステム構成図。

【図２】　本発明の第1の実施形態におけるハードウェア構成図。

【図３】　本発明の第1の実施形態における機能構成図。

【図４】　本発明の第1の実施形態におけるデータ構成図。

【図５】　本発明の第1の実施形態における電子鍵利用処理のフロー図。

【図６】　本発明の第1の実施形態における電子鍵利用処理のフロー図。

【図７】　本発明の第1の実施形態における電子鍵共有処理のフロー図。

【図８】　本発明の第1の実施形態における電子鍵共有時のデータ値の例。

【図９】本発明の第1の実施形態における電子鍵共有時のデータ値の例。

【図１０】本発明の第1の実施形態における電子鍵無効化処理のフロー図。

【図１１】本発明の第1の実施形態における画面表示例。

【図１２】本発明の第２の実施形態におけるデータ構成図。

【図１３】本発明の第２の実施形態における電子鍵購入処理のフロー図。

【図１４】本発明の第２の実施形態における画面表示例。

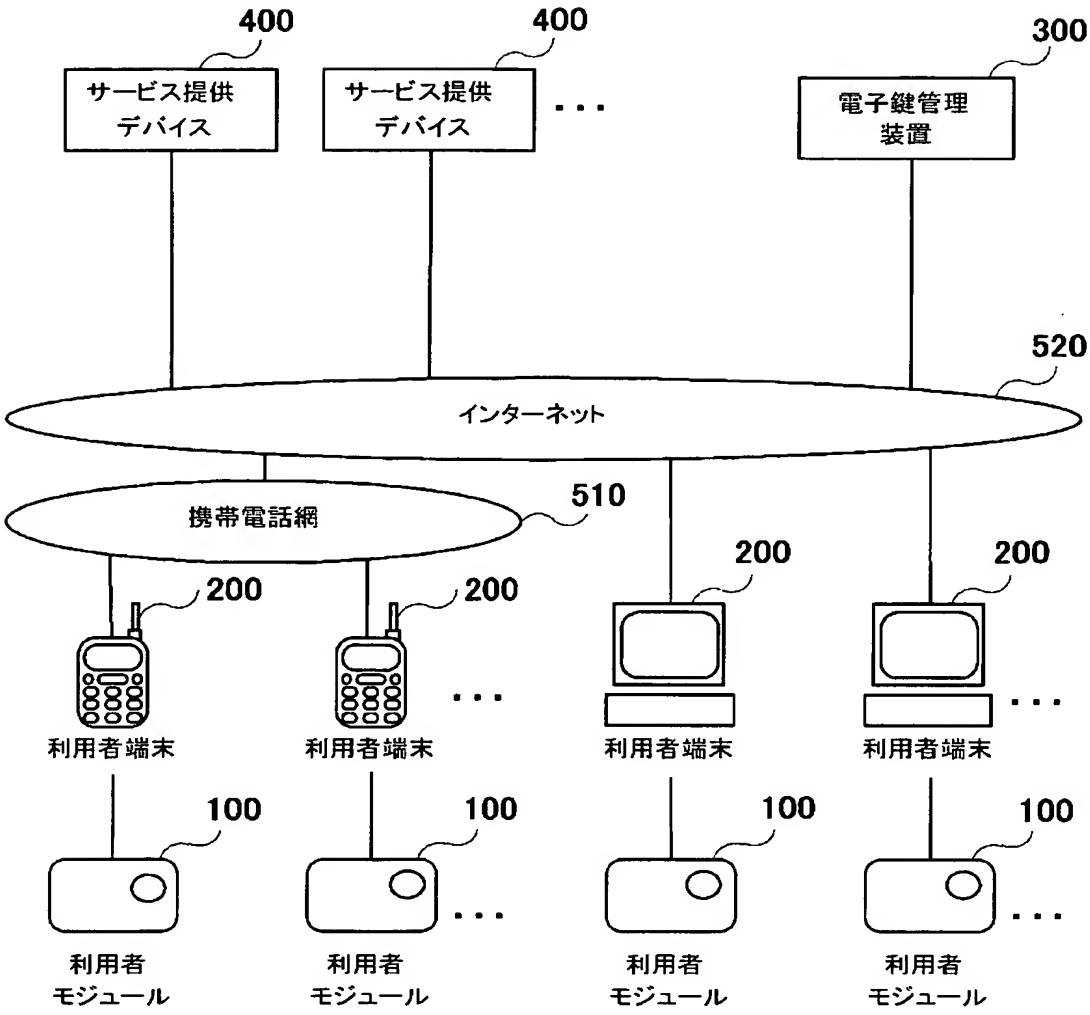
【符号の説明】

１００…利用者モジュール、１１０…ＵＭ認証鍵データ、１２０…利用者鍵テーブル、２００…利用者端末、３００…電子鍵管理装置、３１０…ＳＤ認証鍵データ、３２０…ＵＭ認証鍵データ、３３０…顧客テーブル、４００…サービス提供デバイス、４１０…ＳＤ認証鍵データ、４２０…ＵＭ認証鍵データ、４３０…サービス許可テーブル、４４０…サービス拒否テーブル

【書類名】　図面

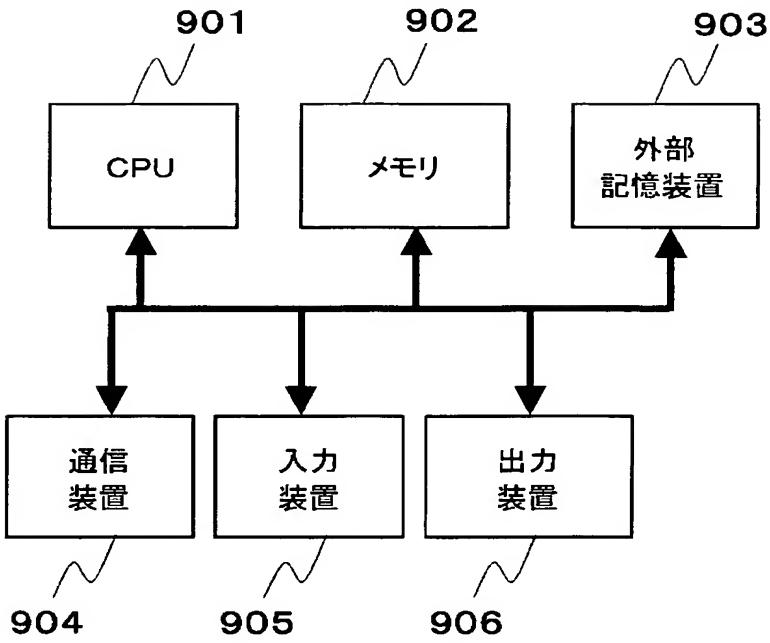
【図１】

図1


400
400
300
サービス提供
デバイス
サービス提供
デバイス
電子鍵管理
装置
520
インターネット
510
携帯電話網
200
200
200
200
利用者端末
利用者端末
利用者端末
利用者端末
100
100
100
100
利用者
モジュール
利用者
モジュール
利用者
モジュール
利用者
モジュール

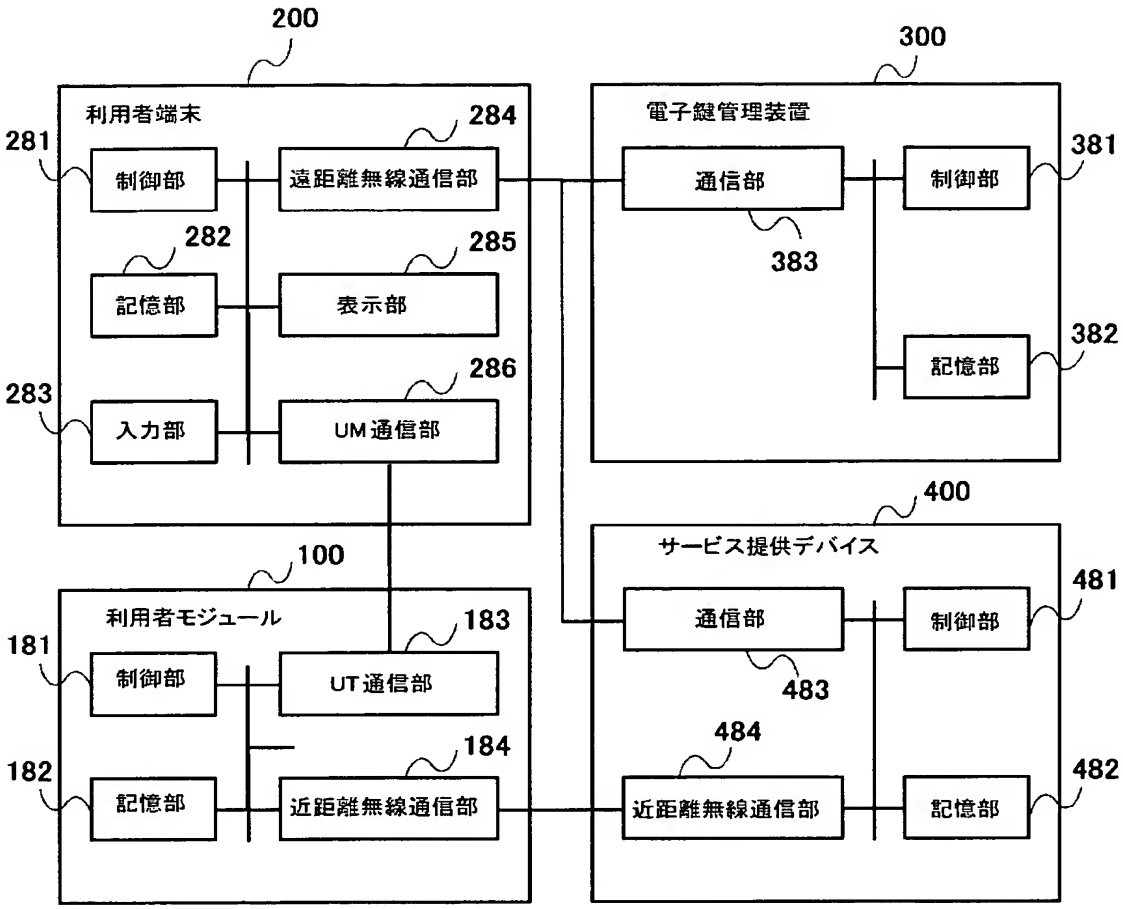
【図２】

図2



【図３】

図3


200
利用者端末
281
制御部
284
遠距離無線通信部
282
記憶部
285
表示部
283
入力部
286
UM通信部
300
電子鍵管理装置
通信部
383
制御部
381
記憶部
382
100
利用者モジュール
181
制御部
183
UT通信部
182
記憶部
184
近距離無線通信部
400
サービス提供デバイス
通信部
483
制御部
481
484
近距離無線通信部
記憶部
482

【図４】

図4

利用者モジュールのデータ

～110
UM認証鍵データ

UM認証鍵
Kauu

～120
利用者電子鍵テーブル

鍵名称	主ID	共有階層	副ID（携帯電話番号）履歴
XX宅	0120040101001	1	XXX-XXX-XXXX
⋮	⋮	⋮	⋮

電子鍵管理装置のデータ

～310
SD認証鍵データ

SD認証鍵
Kaus

～320
UM認証鍵データ

UM認証鍵
Kauu

～330
顧客テーブル

会員番号	パスワード	副 ID(携帯電話番号)	主ID	SDアドレス
001	0001	XXX-XXX-XXXX	20040101001	XXX.XXX.XXX.XXX
002	0002	YYY-YYY-YYYY	20040101002	YYY.YYY.YYY.YYY
⋮	⋮	⋮	⋮	⋮

サービス提供デバイスのデータ

～410
SD認証鍵データ

SD認証鍵
Kaus

～420
UM認証鍵データ

UM認証鍵
Kauu

～430
サービス許可テーブル

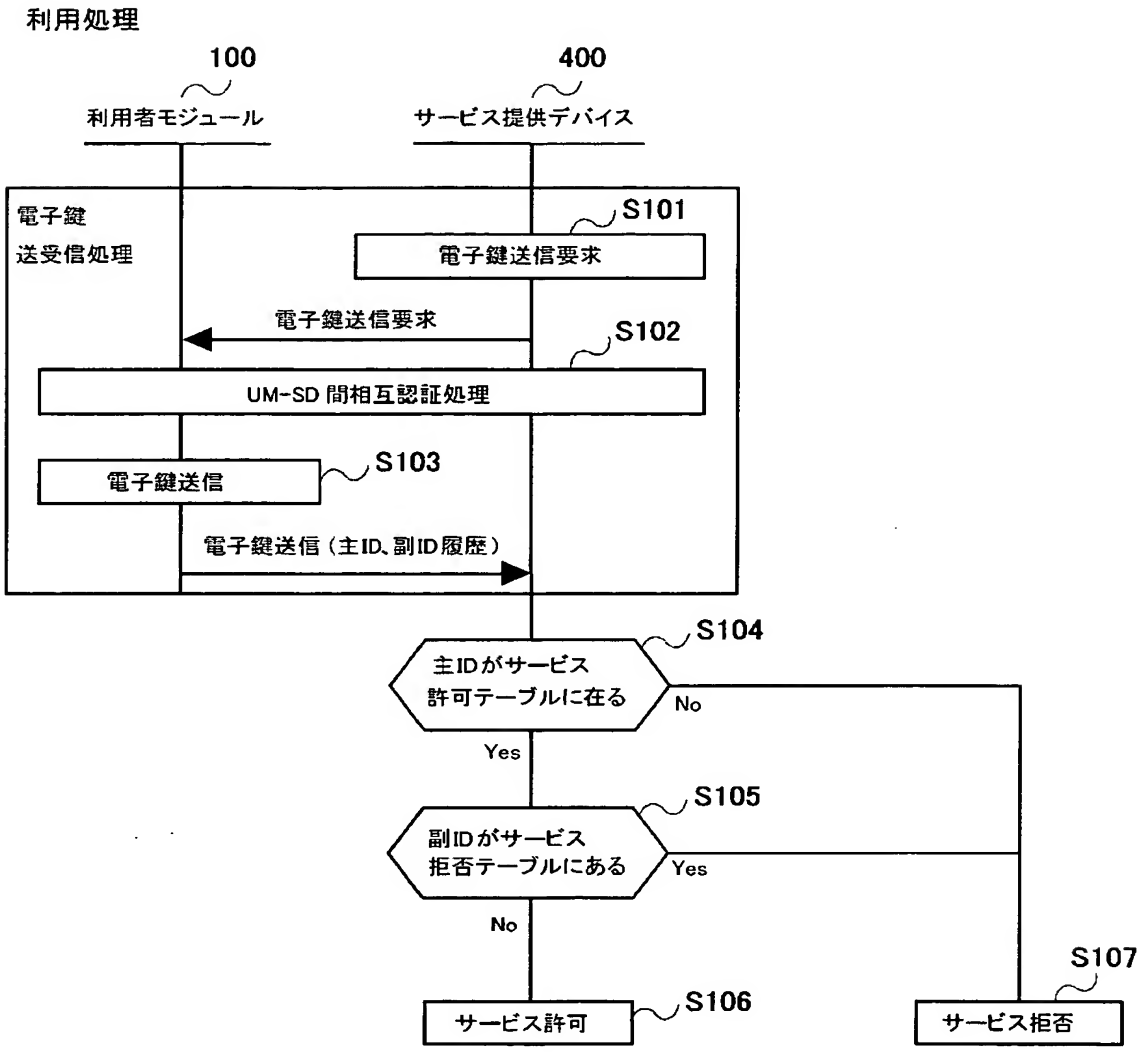
主ID
0120040101001
0120040101002
⋮

～440
サービス拒否テーブル

主ID	副ID
0120040101001	ZZZ-ZZZ-ZZZZ
⋮	⋮

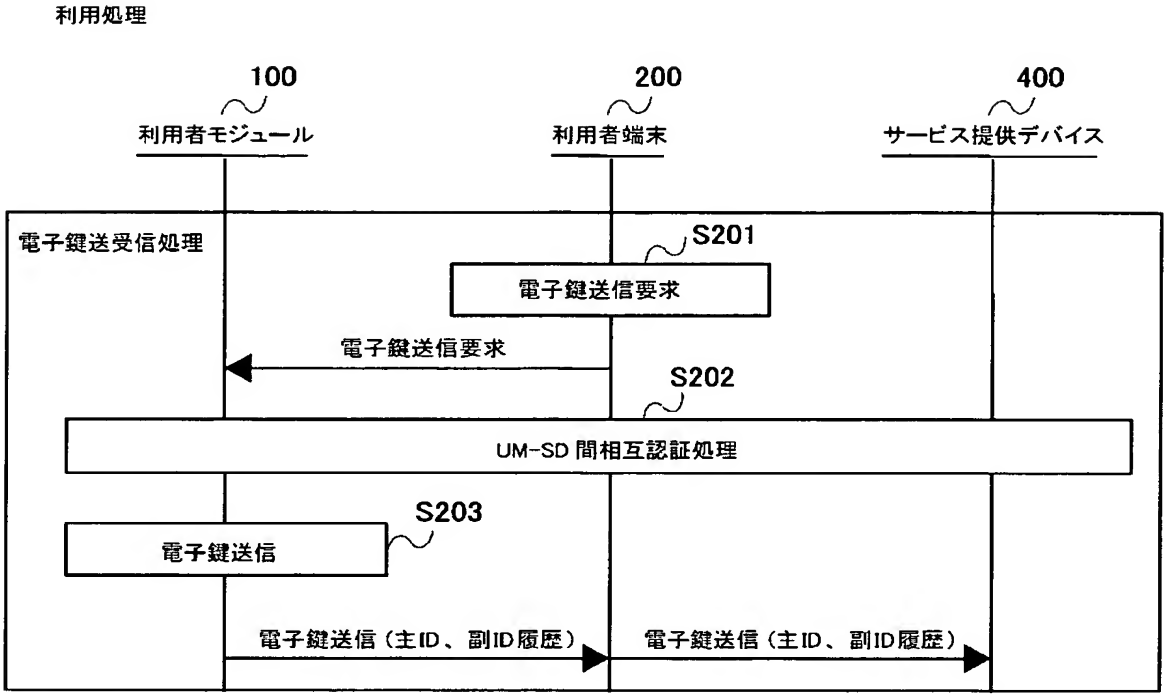
【図５】

図5


利用処理
100
利用者モジュール
400
サービス提供デバイス
電子鍵
送受信処理
S101
電子鍵送信要求
電子鍵送信要求
S102
UM-SD 間相互認証処理
電子鍵送信
S103
電子鍵送信（主ID、副ID履歴）
S104
主IDがサービス
許可テーブルに在る
No
Yes
S105
副IDがサービス
拒否テーブルにある
Yes
No
S107
サービス許可
S106
サービス拒否

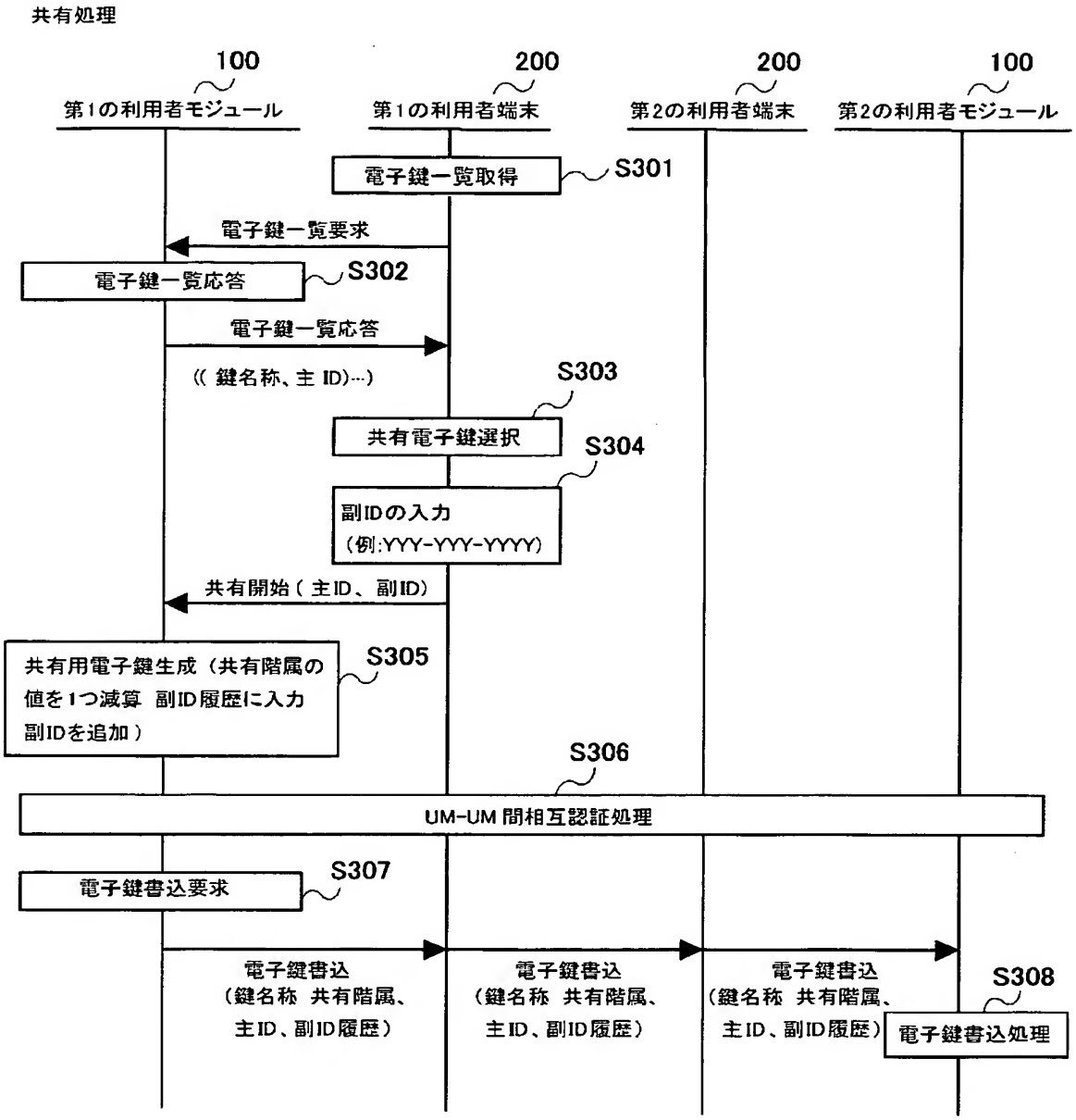
【図６】

図6


利用処理
100
利用者モジュール
200
利用者端末
400
サービス提供デバイス
電子鍵送受信処理
S201
電子鍵送信要求
電子鍵送信要求
S202
UM-SD 間相互認証処理
S203
電子鍵送信
電子鍵送信（主ID、副ID履歴）
電子鍵送信（主ID、副ID履歴）

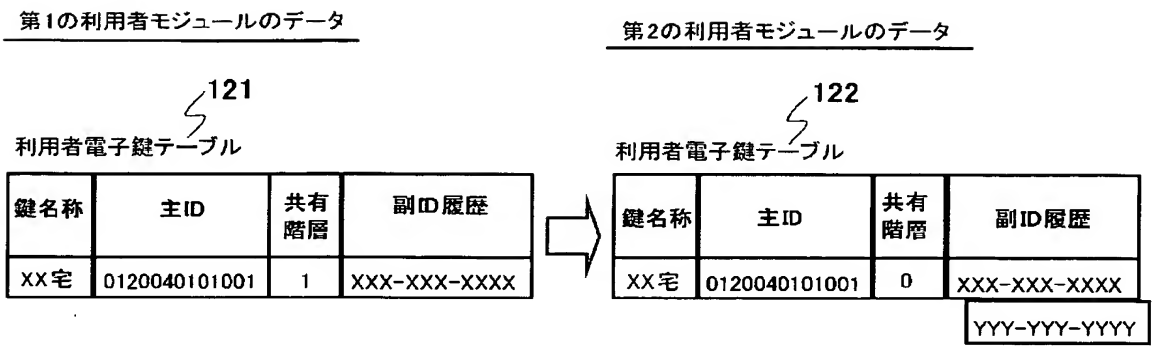
【図７】

図7


共有処理
100
第1の利用者モジュール
200
第1の利用者端末
200
第2の利用者端末
100
第2の利用者モジュール
電子鍵一覧取得
S301
電子鍵一覧要求
電子鍵一覧応答
S302
電子鍵一覧応答
((鍵名称、主 ID)…)
S303
共有電子鍵選択
S304
副IDの入力
(例:YYY-YYY-YYYY)
共有開始 (主ID、副ID)
共有用電子鍵生成（共有階層の値を1つ減算 副ID履歴に入力 副IDを追加 ）
S305
S306
UM-UM 間相互認証処理
電子鍵書込要求
S307
電子鍵書込
(鍵名称 共有階層、主ID、副ID履歴)
電子鍵書込
(鍵名称 共有階層、主ID、副ID履歴)
電子鍵書込
(鍵名称 共有階層、主ID、副ID履歴)
S308
電子鍵書込処理

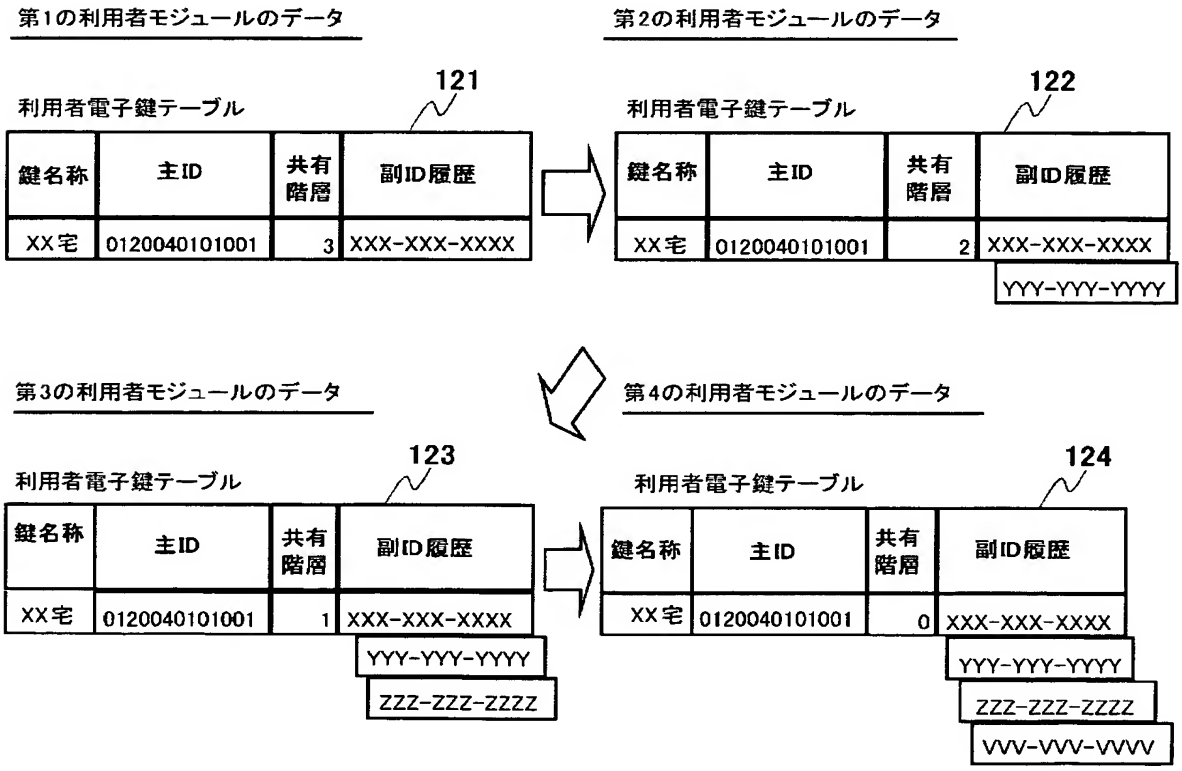
【図８】

図8


第1の利用者モジュールのデータ
121
利用者電子鍵テーブル
鍵名称
主ID
共有階層
副ID履歴
XX宅
0120040101001
1
XXX-XXX-XXXX
第2の利用者モジュールのデータ
122
利用者電子鍵テーブル
鍵名称
主ID
共有階層
副ID履歴
XX宅
0120040101001
0
XXX-XXX-XXXX
YYY-YYY-YYYY

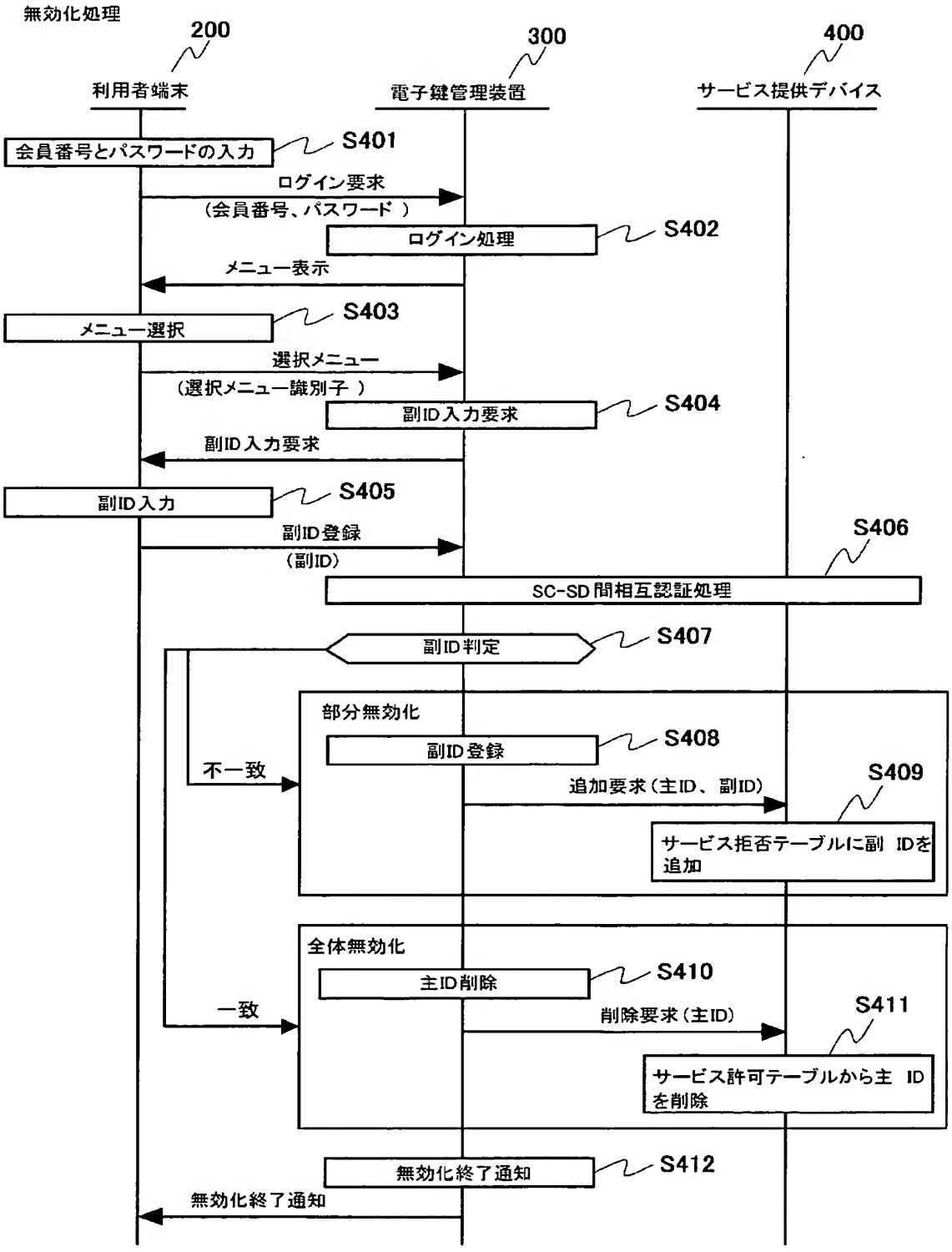
【図９】

図9


第1の利用者モジュールのデータ
121
利用者電子鍵テーブル
鍵名称
主ID
共有階層
副ID履歴
XX宅
0120040101001
3
XXX-XXX-XXXX
第2の利用者モジュールのデータ
122
利用者電子鍵テーブル
鍵名称
主ID
共有階層
副ID履歴
XX宅
0120040101001
2
XXX-XXX-XXXX
YYY-YYY-YYYY
第3の利用者モジュールのデータ
123
利用者電子鍵テーブル
鍵名称
主ID
共有階層
副ID履歴
XX宅
0120040101001
1
XXX-XXX-XXXX
YYY-YYY-YYYY
ZZZ-ZZZ-ZZZZ
第4の利用者モジュールのデータ
124
利用者電子鍵テーブル
鍵名称
主ID
共有階層
副ID履歴
XX宅
0120040101001
0
XXX-XXX-XXXX
YYY-YYY-YYYY
ZZZ-ZZZ-ZZZZ
VVV-VVV-VVVV

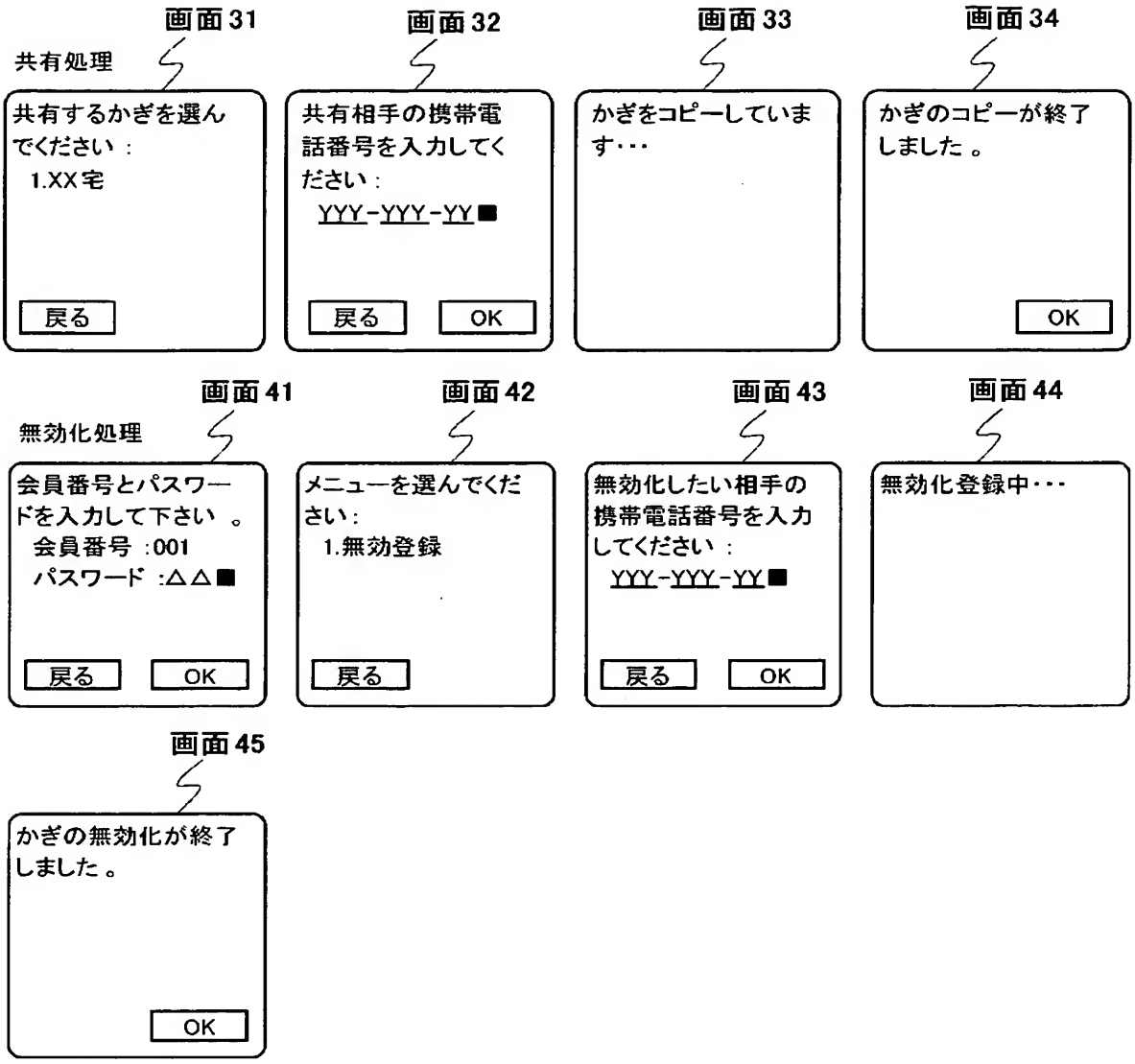
【図１０】

図10


無効化処理
200
利用者端末
300
電子鍵管理装置
400
サービス提供デバイス
会員番号とパスワードの入力
S401
ログイン要求
（会員番号、パスワード）
ログイン処理
S402
メニュー表示
メニュー選択
S403
選択メニュー
（選択メニュー識別子）
副ID入力要求
S404
副ID入力要求
副ID入力
S405
副ID登録
（副ID）
S406
SC-SD間相互認証処理
副ID判定
S407
部分無効化
副ID登録
S408
不一致
追加要求（主ID、副ID）
S409
サービス拒否テーブルに副 IDを追加
全体無効化
主ID削除
S410
一致
削除要求（主ID）
S411
サービス許可テーブルから主 IDを削除
無効化終了通知
S412
無効化終了通知

【図１１】

図11


画面31
共有処理
共有するかぎを選んでください：
1.XX宅
戻る
画面32
共有相手の携帯電話番号を入力してください：
YYY-YYY-YY■
戻る
OK
画面33
かぎをコピーしています・・・
画面34
かぎのコピーが終了しました。
OK
画面41
無効化処理
会員番号とパスワードを入力して下さい。
会員番号：001
パスワード：△△■
戻る
OK
画面42
メニューを選んでください：
1.無効登録
戻る
画面43
無効化したい相手の携帯電話番号を入力してください：
YYY-YYY-YY■
戻る
OK
画面44
無効化登録中・・・
画面45
かぎの無効化が終了しました。
OK

【図１２】

図12

利用者モジュールのデータ

110
UM認証鍵データ

UM認証鍵
Kauu

120
利用者電子鍵テーブル

鍵名称	主ID	共有階層	副ID（携帯電話番号）履歴
車種A	0120040101001	1	XXX-XXX-XXXX
車種B	0120040101002	0	YYY-YYY-YYYY
⋮	⋮	⋮	⋮

電子鍵管理装置のデータ

310
SD認証鍵データ

SD認証鍵
Kaus

320
UM認証鍵データ

UM認証鍵
Kauu

330
顧客テーブル

会員番号	パスワード	副ID（携帯電話番号）
001	0001	XXX-XXX-XXXX
002	0002	YYY-YYY-YYYY
⋮	⋮	⋮

340
取引テーブル

主ID	商品ID	会員番号
0120040101001	001	001
0120040101002	002	002
⋮	⋮	⋮

350
商品テーブル

商品ID	商品名	対応SDアドレス
001	車種A	XXX.XXX.XXX.XXX
002	車種B	YYY.YYY.YYY.YYY
⋮	⋮	⋮

サービス提供デバイスのデータ

410
SD認証鍵データ

SD認証鍵
Kaus

420
UM認証鍵データ

UM認証鍵
Kauu

430
サービス許可テーブル

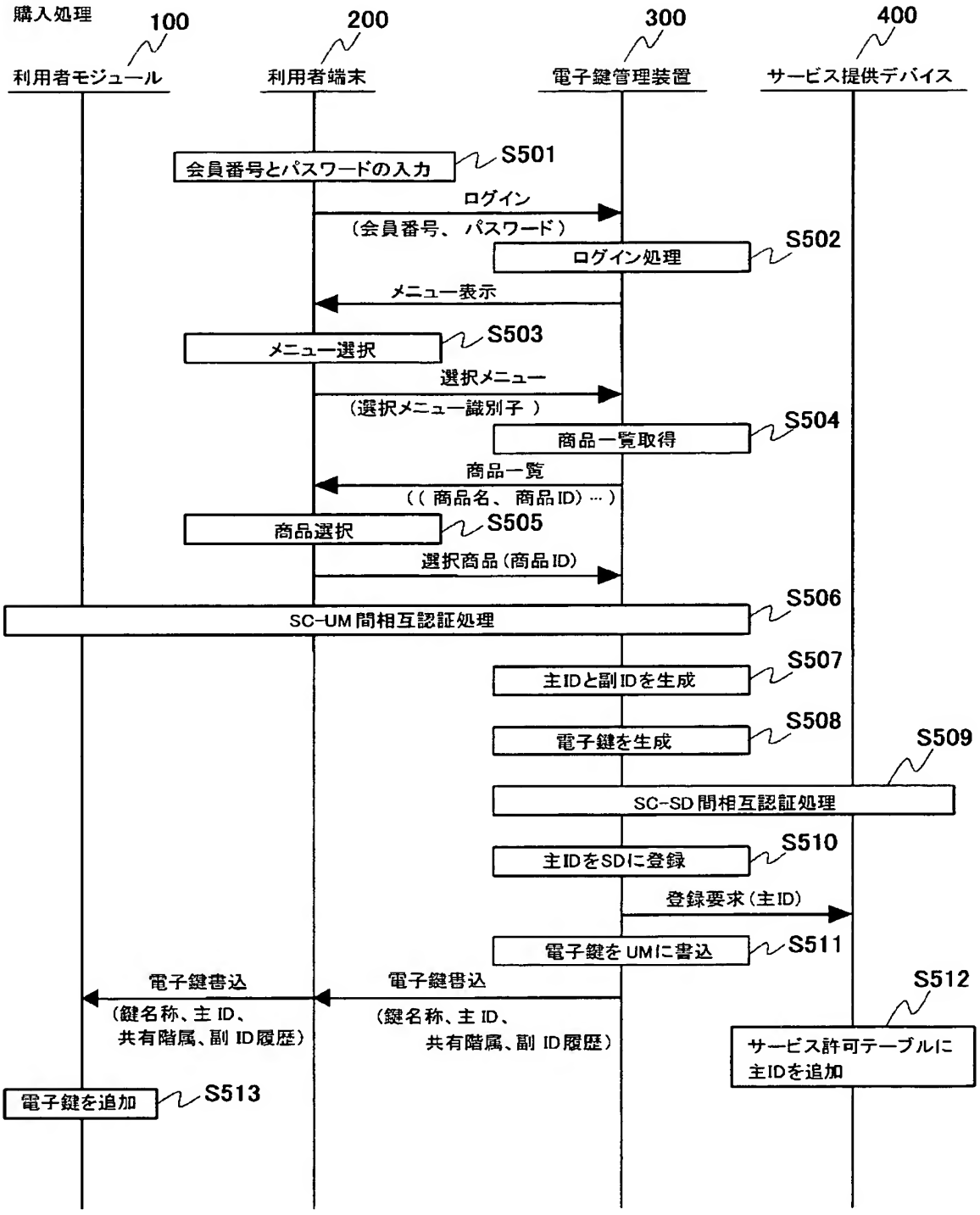
主ID
0120040101001
0120040101002
⋮

440
サービス拒否テーブル

主ID	副ID
0120040101001	ZZZ-ZZZ-ZZZZ
⋮	⋮

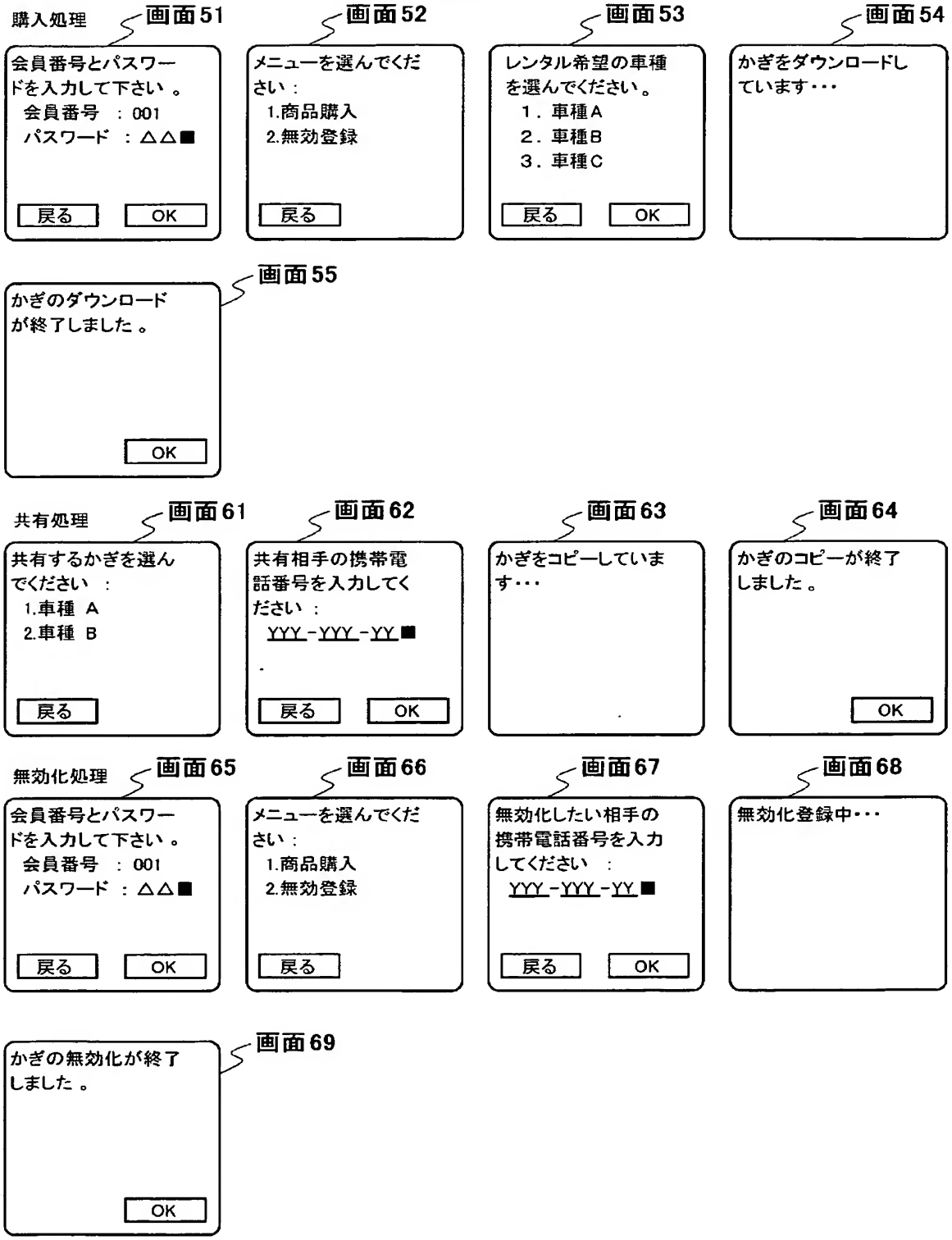
【図１３】

図13


購入処理
100
200
300
400
利用者モジュール
利用者端末
電子鍵管理装置
サービス提供デバイス
会員番号とパスワードの入力
S501
ログイン
（会員番号、パスワード）
ログイン処理
S502
メニュー表示
メニュー選択
S503
選択メニュー
（選択メニュー識別子）
商品一覧取得
S504
商品一覧
（（商品名、商品ID）…）
商品選択
S505
選択商品（商品ID）
SC-UM間相互認証処理
S506
主IDと副IDを生成
S507
電子鍵を生成
S508
SC-SD間相互認証処理
S509
主IDをSDに登録
S510
登録要求（主ID）
電子鍵をUMに書込
S511
電子鍵書込
（鍵名称、主ID、
共有階属、副ID履歴）
電子鍵書込
（鍵名称、主ID、
共有階属、副ID履歴）
S512
サービス許可テーブルに
主IDを追加
電子鍵を追加
S513

【図１４】

図14


購入処理
画面51
会員番号とパスワードを入力して下さい。
会員番号　：001
パスワード　：△△■
戻る
OK
画面52
メニューを選んでください：
1.商品購入
2.無効登録
戻る
画面53
レンタル希望の車種を選んでください。
１．車種A
２．車種B
３．車種C
戻る
OK
画面54
かぎをダウンロードしています・・・
画面55
かぎのダウンロードが終了しました。
OK
共有処理
画面61
共有するかぎを選んでください：
1.車種 A
2.車種 B
戻る
画面62
共有相手の携帯電話番号を入力してください：
YYY-YYY-YY■
戻る
OK
画面63
かぎをコピーしています・・・
画面64
かぎのコピーが終了しました。
OK
無効化処理
画面65
会員番号とパスワードを入力して下さい。
会員番号　：001
パスワード　：△△■
戻る
OK
画面66
メニューを選んでください：
1.商品購入
2.無効登録
戻る
画面67
無効化したい相手の携帯電話番号を入力してください：
YYY-YYY-YY■
戻る
OK
画面68
無効化登録中・・・
画面69
かぎの無効化が終了しました。
OK

【書類名】　要約書

【要約】

【課題】複数の利用者で共有電子鍵によりサービスを共同利用する場合に、一部の人だけの電子鍵を無効化する方法を提供する。

【解決手段】利用者の保有する利用者モジュール１００に格納する電子鍵データは、主ＩＤデータと副ＩＤ履歴データの２つのデータを有する。サービス提供デバイス４００は、サービス許可テーブルとサービス拒否テーブルの２つのテーブルを保持し、電子鍵データを利用者モジュール１００から受信したときに、電子鍵の主ＩＤデータがサービス許可テーブルに存在し（ステップ１０４）、かつ副ＩＤ履歴データに含まれる副ＩＤデータがサービス拒否テーブルに存在しない場合のみ（ステップ１０５）、サービス利用を許可する（ステップ１０６）。

【選択図】　図５

特願２００３－１１８１２６

出　願　人　履　歴　情　報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所